

TQ7403-R

WI-FI 6E (802.11AX) WIRELESS AP ROUTER



Command Reference for AlliedWare Plus™ Version 5.5.5-2.1

Acknowledgments

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

Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California. #
All rights reserved.

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

Copyright (c) 1998-2019 The OpenSSL Project#

Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson#

All rights reserved.

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

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

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

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

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

GPL Code Request

Allied Telesis Labs (Ltd)

PO Box 8011

Christchurch

New Zealand

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

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

Contents

Preface:	Acknowledgments.....	ii
PART 1:	Setup and Troubleshooting.....	33
Chapter 1:	CLI Navigation Commands.....	34
	Introduction.....	35
	configure terminal.....	36
	disable (Privileged Exec mode).....	37
	do.....	38
	enable (Privileged Exec mode).....	39
	end.....	41
	exit.....	42
	help.....	43
	logout.....	44
	show history.....	45
Chapter 2:	Device GUI and Vista Manager EX Commands.....	46
	Introduction.....	47
	atmf topology-gui enable.....	48
	gui preference flash.....	50
	http check-api-content-type-header.....	51
	http client vrf.....	52
	http log webapi-requests.....	53
	http port.....	54
	http secure-port.....	56
	http tls-version-minimum.....	58
	http trustpoint.....	59
	http vrf.....	61
	log event-host.....	62
	service http.....	63
	show http.....	64
	show http client.....	65
	update webgui now.....	66
Chapter 3:	File and Configuration Management Commands.....	67

Introduction.....	69
boot config-file.....	71
boot config-file backup.....	72
boot system.....	73
boot system backup.....	74
cd.....	75
copy (filename).....	76
copy debug.....	78
copy running-config.....	79
copy startup-config.....	80
copy zmodem.....	81
crypto verify.....	82
crypto verify bootrom.....	84
crypto verify signed.....	86
delete.....	87
delete debug.....	88
dir.....	89
edit.....	91
erase factory-default.....	93
erase startup-config.....	94
ip tftp source-interface.....	95
ip tftp vrf.....	96
ipv6 tftp source-interface.....	97
mkdir.....	98
move.....	99
move debug.....	100
pwd.....	101
rmdir.....	102
show boot.....	103
show hash.....	105
show file.....	106
show file systems.....	107
show running-config.....	110
show running-config interface.....	114
show running-config unencrypted.....	117
show startup-config.....	118
show version.....	119
strict-user-process-control.....	120
strict-user-process-control force.....	121
write file.....	122
write memory.....	123
write terminal.....	124

Chapter 4: User Access Commands..... 125

Introduction.....	127
aaa authentication enable default local.....	128
aaa local authentication attempts lockout-time.....	129
aaa local authentication attempts max-fail.....	130
aaa login fail-delay.....	132
clear aaa local user lockout.....	133
clear line console.....	134
clear line vty.....	135
enable password.....	136
enable secret (deprecated).....	138
exec-timeout.....	139
flowcontrol hardware (asyn/console).....	141

length (asyn).....	143
line.....	145
privilege level.....	147
security-password history.....	148
security-password forced-change.....	149
security-password lifetime.....	150
security-password min-lifetime-enforce.....	151
security-password minimum-categories.....	153
security-password minimum-length.....	155
security-password reject-expired-pwd.....	156
security-password warning.....	158
service advanced-vty.....	159
service password-encryption.....	160
service telnet.....	161
show aaa local user locked.....	162
show privilege.....	164
show security-password configuration.....	165
show security-password user.....	166
show telnet.....	167
show users.....	168
strict-user-process-control.....	169
strict-user-process-control force.....	170
telnet server.....	171
terminal length.....	172
terminal resize.....	173
username.....	174

Chapter 5: Update Manager Commands.....178

Introduction.....	179
show resource.....	180
update now.....	181
update webgui now.....	182

Chapter 6: System Configuration and Monitoring Commands.....183

Introduction.....	185
banner display external-manager.....	186
banner exec.....	187
banner external-manager.....	189
banner login (system).....	191
banner motd.....	192
clock set.....	194
clock summer-time date.....	195
clock summer-time recurring.....	197
clock timezone.....	200
debug core-file.....	201
findme.....	202
hostname.....	203
low-memory restart.....	205
max-fib-routes.....	206
max-static-routes.....	208
no debug all.....	209
reboot.....	211
receive-packet-scheduler.....	212
reload.....	214
show banner external-manager.....	215

show clock.....	216
show cpu.....	218
show cpu history.....	221
show debugging.....	223
show interface memory.....	224
show memory.....	226
show memory allocations.....	229
show memory history.....	231
show memory pools.....	232
show memory shared.....	233
show process.....	234
show reboot history.....	237
show router-id.....	238
show system.....	239
show system environment.....	240
show system environment counters.....	241
show system interrupts.....	243
show system mac.....	244
show system pci device.....	245
show system pci tree.....	246
show system serialnumber.....	247
show tech-support.....	248
speed (asyn).....	251
terminal monitor.....	253
undebg all.....	254

Chapter 7: Logging Commands.....255

Introduction.....	257
clear exception log.....	258
clear log.....	259
clear log buffered.....	260
clear log permanent.....	261
connection-log events.....	262
copy buffered-log.....	263
copy permanent-log.....	264
default log buffered.....	265
default log console.....	266
default log email.....	267
default log host.....	268
default log monitor.....	269
default log permanent.....	270
log buffered.....	271
log buffered (filter).....	272
log buffered exclude.....	277
log buffered size.....	281
log console.....	282
log console (filter).....	283
log console exclude.....	288
log date-format.....	292
log email.....	294
log email (filter).....	295
log email exclude.....	300
log email time.....	304
log facility.....	306
log host.....	308
log host (filter).....	310

	log host exclude.....	315
	log host source.....	320
	log host startup-delay.....	321
	log host time.....	323
	log monitor (filter).....	326
	log monitor exclude.....	331
	log permanent.....	335
	log permanent (filter).....	336
	log permanent exclude.....	341
	log permanent size.....	345
	log-rate-limit nsm.....	346
	log trustpoint.....	348
	log url-requests.....	350
	show connection-log events.....	351
	show counter log.....	352
	show exception log.....	354
	show log.....	355
	show log config.....	357
	show log permanent.....	360
	show running-config log.....	362
Chapter 8:	Scripting Commands.....	363
	Introduction.....	364
	activate.....	365
	echo.....	367
	wait.....	368
Chapter 9:	Interface Commands.....	369
	Introduction.....	370
	description (interface).....	371
	interface (to configure).....	372
	ip tcp adjust-mss.....	374
	ipv6 tcp adjust-mss.....	376
	mtu.....	378
	service statistics interfaces counter.....	380
	show interface.....	381
	show interface brief.....	384
	show interface memory.....	386
	show interface status.....	388
	shutdown.....	390
Chapter 10:	Wireless Commands.....	391
	Introduction.....	395
	3gpp-info (wireless-network-passpoint-dot11u).....	396
	additional-step-required enable (wireless-network-passpoint-dot11u).....	397
	airtime-fairness mode (wireless-ap-prof-radio).....	398
	airtime-percentage.....	400
	anqp-domain-id (wireless-network-passpoint-hs20).....	402
	anqp-element (wireless-network-passpoint-dot11u).....	403
	antenna (wireless-ap-prof-radio).....	404
	ap local.....	405
	ap-profile local.....	406
	association-advertisement enable.....	407
	atmf-application-proxy port enable.....	408
	authentication (wireless-sec-wep).....	409

auto-discovery disable.....	410
band-steering (wireless-network).....	411
bandwidth (wireless-ap-prof-radio).....	412
bcast-key-refresh-interval (wireless-sec-wpa-ent).....	413
bcast-key-refresh-interval (wireless-sec-wpa-psnl).....	414
bss-trans-manage enable.....	415
captive-portal.....	416
captive-portal virtual-ip.....	417
channels (wireless-ap-prof-radio).....	418
channel (wireless-ap-radio).....	419
ciphers (wireless-sec-wpa-ent).....	420
ciphers (wireless-sec-wpa-psnl).....	421
client-isolation-mode.....	422
conn-capability protocol (wireless-network-passpoint-hs20).....	423
country-code.....	425
deauth-req-timeout (wireless-network-passpoint-hs20).....	426
debug wireless.....	427
description (wireless-ap).....	430
description (wireless-ap-prof).....	431
description (wireless-mac-flt).....	432
description (wireless-network).....	433
description (wireless-sc-prof).....	434
dgaf enable (wireless-network-passpoint-hs20).....	435
domain-name (wireless-network-passpoint-dot11u).....	436
dot11u (wireless-network-passpoint).....	437
dtim-period.....	438
dup-auth-received (wireless-network).....	439
emergency-service-reachable enable (wireless-network-passpoint-dot11u).....	440
enable (wireless-ap-prof-radio).....	441
enable (wireless-network-cp).....	442
enable (wireless-network-passpoint).....	443
external-page-url.....	444
force-disable (wireless-ap-radio).....	445
gas-address-behavior (wireless-network-passpoint-dot11u).....	446
gas-comeback-delay (wireless-network-passpoint-dot11u).....	447
hessid (wireless-network-passpoint-dot11u).....	448
hide-ssid (wireless-network).....	450
hs20 (wireless-network-passpoint).....	451
inactivity-timer.....	452
index.....	453
initialization-button enable.....	454
internet-access enable (wireless-network-passpoint-dot11u).....	455
ip-addr-type-availability (wireless-network-passpoint-dot11u).....	456
key (wireless-sc-prof).....	458
key (wireless-sec-wep).....	459
key (wireless-sec-wpa-psnl).....	461
l2tif enable (wireless-network-passpoint-hs20).....	462
led enable.....	463
legacy-rates.....	464
length (wireless-sec-wep).....	466
mac-auth dynamic-vlan enable.....	467
mac-auth mode.....	469
mac-auth two-step-auth-with-cp enable.....	470
mac-auth password.....	471
mac-auth radius auth group (wireless-network).....	472
mac-auth radius dynamic-authorization-client.....	473
mac-auth radius send service-type.....	474

mac-auth username.....	475
management-frame-protection enable (wireless-sec-wpa-ent).....	477
management-frame-protection enable (wireless-sec-wpa-psnl).....	479
max-clients.....	481
mode (wireless-ap-prof-radio).....	482
multicast-to-unicast enable.....	484
multicast-tx-rate.....	485
mode (wireless-network-cp).....	487
nai-realm (wireless-network-passpoint-dot11u).....	489
neighbor-ap-detection enable.....	491
network-auth-type (wireless-network-passpoint-dot11u).....	492
network-type (wireless-network-passpoint-dot11u).....	494
network (wireless).....	496
operating-class (wireless-network-passpoint-hs20).....	497
operator (wireless-network-passpoint-hs20).....	498
page-proxy-url.....	499
passpoint.....	500
power (wireless-ap-radio).....	501
pre-authentication enable (wireless-sec-wpa-ent).....	502
proxy-arp enable.....	503
proxy-arp-through enable.....	504
qos-map-set (wireless-network-passpoint-dot11u).....	505
radio (wireless-ap).....	506
radio (wireless-ap-profile).....	507
radius accounting enable.....	508
radius auth group (wireless-network-cp).....	509
radius auth group (wireless-sec-wpa-ent).....	511
redirect-url.....	512
roaming-oi (wireless-network-passpoint-dot11u).....	513
rts-threshold.....	514
rule (wireless-mac-filter).....	515
sc-profile.....	516
security (wireless).....	517
security (wireless-network).....	519
session-keep.....	520
session-key-refresh-action.....	521
session-key-refresh-interval.....	522
session-timeout-action (wireless network-cp).....	523
session-timeout-interval (wireless network-cp).....	524
show debugging wireless.....	525
show wireless.....	526
show wireless ap.....	527
show wireless ap capability.....	529
show wireless ap clients.....	532
show wireless ap counter.....	533
show wireless ap neighbors.....	534
show wireless ap-profile.....	535
show wireless captive-portal network walled-garden.....	537
show wireless country-code.....	538
show wireless network.....	539
show wireless security.....	543
show wireless wireless-mac-filter.....	545
single-channel-scan enable.....	547
single-channel-scan duration.....	548
single-channel-scan interval.....	549
single-channel-scan keep-data-time.....	550
smart-connect-profile.....	551

ssid (wireless-network).....	552
ssid (wireless-sc-prof).....	553
station-isolation enable (wireless-ap-prof-radio).....	554
type (wireless-sec-wep).....	556
unauth-emergency-service-access enable (wireless-network-passpoint-dot11u).....	557
unassociated-client-list acquire.....	558
vap (wireless-ap-prof-radio).....	559
versions (wireless-sec-wpa-ent).....	560
versions (wireless-sec-wpa-psnl).....	561
vlan (wireless-network).....	562
walled-garden-dns-proxy enable.....	563
walled-garden entry.....	564
wan-metrics downlink-load (wireless-network-passpoint-hs20).....	566
wan-metrics downlink-speed (wireless-network-passpoint-hs20).....	567
wan-metrics info (wireless-network-passpoint-hs20).....	568
wan-metrics load-measure-duration (wireless-network-passpoint-hs20).....	570
wan-metrics uplink-load (wireless-network-passpoint-hs20).....	571
wan-metrics uplink-speed (wireless-network-passpoint-hs20).....	572
web-auth radius auth group.....	573
wireless.....	574
wireless ap-configuration apply ap local.....	575
wireless ap-configuration pull ap.....	576
wireless disassociate ap local client.....	577
wireless export.....	578
wireless import.....	579
wireless-mac-filter (wireless).....	580
wireless-mac-filter-id.....	581
wireless-mac-filter (wireless-ap-prof).....	583
wireless-mac-filter enable.....	585

PART 2: Interfaces and Layer 2..... 586

Chapter 11: Bridging Commands..... 587

Introduction.....	588
ageing-time.....	589
bridge.....	590
bridge-group.....	591
l3-filtering enable.....	593
mac-learning.....	594
show bridge.....	595
show bridge macaddr.....	597

Chapter 12: Ethernet Bonding..... 598

Introduction.....	599
aggregator-type.....	600
bond.....	601
bond-group.....	602
show bond.....	603
show bond info.....	604

Chapter 13: 802.1Q Encapsulation Commands..... 605

Introduction.....	606
encapsulation dot1q.....	607

Chapter 14:	PPP Commands.....	609
	Introduction.....	610
	debug ppp.....	611
	encapsulation ppp.....	614
	interface (PPP).....	615
	ip address negotiated.....	616
	ip tcp adjust-mss.....	618
	ip unnumbered.....	620
	ipv6 tcp adjust-mss.....	622
	keepalive (PPP).....	624
	mtu (PPP).....	626
	peer default ip address.....	628
	peer neighbor-route.....	630
	ppp authentication.....	632
	ppp authentication refuse.....	634
	ppp hostname.....	636
	ppp ipcp dns.....	638
	ppp ipcp dns suffix-list.....	640
	ppp ipcp ip-override.....	642
	ppp password.....	643
	ppp service-name (PPPoE).....	645
	ppp timeout idle.....	646
	ppp username.....	647
	show debugging ppp.....	648
	show interface (PPP).....	649
	undebg ppp.....	652
Chapter 15:	PPP over Ethernet (PPPoE) Commands.....	654
	Introduction.....	655
	client (pppoe-relay).....	656
	max-sessions.....	657
	pppoe-relay.....	658
	server (pppoe-relay).....	659
	show running-config pppoe-relay.....	660
	timeout (pppoe-relay).....	661
PART 3:	Routing.....	663
Chapter 16:	IP Addressing and Protocol Commands.....	664
	Introduction.....	665
	arp.....	666
	arp log.....	668
	arp opportunistic-nd.....	672
	arp-loose-check.....	674
	arp-reply-bc-dmac.....	676
	clear arp-cache.....	677
	debug ip packet interface.....	679
	ip address (IP Addressing and Protocol).....	682
	ip directed-broadcast.....	684
	ip forwarding.....	686
	ip forward-protocol udp.....	687
	ip helper-address.....	689
	ip icmp error-interval.....	691

ip icmp-timestamp.....	692
ip limited-local-proxy-arp.....	693
ip local-proxy-arp.....	694
ip proxy-arp.....	696
ip redirects.....	697
ip tcp synack-retries.....	698
ip tcp timeout established.....	699
ip tcp-timestamp.....	700
ip unreachable.....	701
local-proxy-arp.....	704
ping.....	705
show arp.....	708
show debugging ip packet.....	711
show ip flooding-next hops.....	713
show ip forwarding.....	714
show ip interface.....	715
show ip interface vrf.....	716
show ip sockets.....	718
show ip traffic.....	722
tcpdump.....	724
traceroute.....	725
undebg ip packet interface.....	726

Chapter 17: Domain Name Service (DNS) Commands.....727

Introduction.....	729
accept-invalid-sslcert.....	730
clear ip dns forwarding cache.....	731
custom-failure.....	732
custom-success.....	733
ddns enable.....	734
ddns-update-method.....	735
ddns-update now.....	737
debug ddns.....	738
debug ip dns forwarding.....	739
description (domain-list).....	740
domain.....	741
expect-html-response.....	742
follow-redirects.....	743
get-before-submit.....	744
get-params.....	745
host-name (ddns-update-method).....	746
ip ddns-update-method.....	747
ip dns forwarding.....	748
ip dns forwarding cache.....	750
ip dns forwarding dead-time.....	752
ip dns forwarding domain-list.....	753
ip dns forwarding retry.....	755
ip dns forwarding source-interface.....	756
ip dns forwarding timeout.....	757
ip domain-list.....	758
ip domain-lookup.....	759
ip domain-name.....	761
ip name-server.....	762
ip name-server preferred-order.....	765
ipv6 ddns-update-method.....	767
obey-form.....	768

password (ddns-update-method).....	769
ppp ipcp dns.....	770
ppp ipcp dns suffix-list.....	772
retry-interval.....	774
show ddns-update-method status.....	776
show debugging ip dns forwarding.....	777
show hosts.....	778
show ip dns forwarding.....	780
show ip dns forwarding cache.....	781
show ip dns forwarding server.....	783
show ip domain-list.....	785
show ip domain-name.....	786
show ip name-server.....	787
suppress-ipv4-updates.....	789
undebg ddns.....	790
update-interval (ddns-update-method).....	791
update-url (ddns-update-method).....	792
use-ipv4-for-ipv6-updates.....	795
username (ddns-update-method).....	796

Chapter 18: IPv6 Commands.....797

Introduction.....	798
clear ipv6 neighbors.....	799
ipv6 address.....	800
ipv6 address autoconfig.....	802
ipv6 address suffix.....	804
ipv6 enable.....	805
ipv6 eui64-linklocal.....	807
ipv6 forwarding.....	808
ipv6 icmp error-interval.....	809
ipv6 nd accept-ra-default-routes.....	810
ipv6 nd accept-ra-pinfo.....	811
ipv6 nd current-hoplimit.....	812
ipv6 nd dns search-list.....	814
ipv6 nd dns-server.....	815
ipv6 nd managed-config-flag.....	817
ipv6 nd minimum-ra-interval.....	819
ipv6 nd other-config-flag.....	821
ipv6 nd prefix.....	822
ipv6 nd proxy interface.....	825
ipv6 nd ra-interval.....	826
ipv6 nd ra-lifetime.....	827
ipv6 nd reachable-time.....	829
ipv6 nd retransmission-time.....	831
ipv6 nd route-information.....	833
ipv6 nd router-preference.....	835
ipv6 nd suppress-ra.....	836
ipv6 opportunistic-nd.....	837
ipv6 route.....	838
ipv6 route vrf.....	840
ipv6 unreachable.....	843
ping ipv6.....	845
show ipv6 forwarding.....	848
show ipv6 interface.....	849
show ipv6 neighbors.....	851
show ipv6 route.....	852

show ipv6 route summary.....	855
traceroute ipv6.....	856

Chapter 19: Routing Commands..... 857

Introduction.....	858
ip route.....	859
ipv6 route.....	863
ipv6 route vrf.....	865
max-fib-routes.....	868
max-static-routes.....	870
maximum-paths.....	871
show ip route.....	872
show ip route database.....	875
show ip route summary.....	877
show ipv6 route.....	879
show ipv6 route summary.....	882

Chapter 20: VRF-lite Commands..... 883

Introduction.....	885
arp.....	886
arp opportunistic-nd.....	888
clear arp-cache.....	890
crypto key pubkey-chain knownhosts.....	892
description (VRF).....	894
export map.....	895
http client vrf.....	896
http vrf.....	897
import map.....	898
ip route static inter-vrf.....	899
ip route vrf.....	900
ip tftp vrf.....	904
ip vrf.....	905
ip vrf forwarding.....	906
log host.....	907
log host exclude.....	909
log host (filter).....	914
log host time.....	919
max-fib-routes (VRF).....	922
max-static-routes (VRF).....	924
ping.....	925
radius-server host.....	928
show arp.....	933
show crypto key pubkey-chain knownhosts.....	936
show http client.....	938
show ip interface vrf.....	939
show ip route.....	941
show ip route database.....	944
show ip route summary.....	946
show ip vrf.....	948
show ip vrf detail.....	949
show ip vrf interface.....	950
show running-config vrf.....	951
snmp-server host.....	952
snmp-server vrf.....	955
ssh.....	956

ssh client.....	959
ssh client vrf.....	962
ssh server vrf.....	963
tacacs-server host.....	964
tcpdump.....	967
telnet.....	968
traceroute.....	970
vrf.....	971

PART 4: Access and Security.....973

Chapter 21: Traffic Control Commands..... 974

Introduction.....	975
class (htb).....	976
class (priority).....	979
class (wrr).....	981
debug traffic-control.....	983
interface (traffic-control).....	984
interface dynamic-virtual-bandwidth.....	986
l3-filtering enable.....	988
move rule (traffic-control).....	989
policy (traffic-control).....	990
red-curve.....	992
rule (traffic-control).....	994
show debugging traffic-control.....	996
show running-config traffic-control.....	997
show traffic-control counters.....	998
show traffic-control interface.....	1000
show traffic-control policy.....	1001
show traffic-control red-curve.....	1004
show traffic-control rule config-check.....	1006
show traffic-control rule.....	1007
show traffic-control.....	1008
sub-class (htb).....	1009
sub-class (priority).....	1011
sub-class (wrr).....	1013
sub-sub-class (htb).....	1015
sub-sub-class (priority).....	1017
sub-sub-class (wrr).....	1019
traffic-control enable.....	1021
traffic-control.....	1022

Chapter 22: AAA Commands..... 1024

Introduction.....	1025
aaa accounting commands.....	1026
aaa accounting login.....	1028
aaa accounting openvpn.....	1031
aaa accounting update.....	1033
aaa authentication 2fa-registration default group.....	1035
aaa authentication download-portal.....	1037
aaa authentication enable default group tacacs+.....	1039
aaa authentication enable default local.....	1042
aaa authentication isakmp.....	1043
aaa authentication login.....	1044
aaa authentication openvpn.....	1047

aaa authorization commands.....	1050
aaa authorization config-commands.....	1052
aaa group server.....	1053
aaa local authentication attempts lockout-time.....	1055
aaa local authentication attempts max-fail.....	1056
aaa local authentication attempts max-fail remote-login-only.....	1058
aaa login fail-delay.....	1059
accounting login.....	1060
authorization commands.....	1061
clear aaa local user lockout.....	1063
debug aaa.....	1064
login authentication.....	1065
proxy-port.....	1066
radius-secure-proxy aaa.....	1067
server (radsecproxy-aaa).....	1068
server mutual-authentication.....	1070
server name-check.....	1071
server trustpoint.....	1072
show aaa local user locked.....	1074
show aaa server group.....	1076
show debugging aaa.....	1077
show radius server group.....	1078
undebg aaa.....	1080

Chapter 23: Lightweight Directory Access Protocol (LDAP) Commands...1081

Introduction.....	1082
authentication (ldap-server).....	1083
base-dn.....	1085
bind authenticate root-dn.....	1087
deadtime (ldap-server).....	1088
debug ldap client.....	1089
group-attribute.....	1091
group-dn.....	1092
host (ldap-server).....	1093
ldap-server.....	1095
login-attribute.....	1097
port (ldap-server).....	1099
retransmit (ldap-server).....	1101
search-filter.....	1102
secure cipher (ldap-server).....	1104
secure mode (ldap-server).....	1106
secure trustpoint (ldap-server).....	1108
server (ldap-group).....	1109
show ldap server group.....	1110
timeout (ldap-server).....	1112

Chapter 24: RADIUS Commands.....1113

Introduction.....	1114
auth-mac-promiscuous.....	1115
deadtime (RADIUS server group).....	1116
debug radius.....	1117
ip radius require-message-authenticator.....	1118
ip radius source-interface.....	1119
radius-server deadtime.....	1120
radius-server host.....	1121

radius-server key.....	1126
radius-server retransmit.....	1128
radius-server timeout.....	1130
server (RADIUS server group).....	1132
show debugging radius.....	1135
show radius.....	1136
show radius local-server auth-mac-promiscuous.....	1139
undebg radius.....	1140

Chapter 25: Local RADIUS Server Commands..... 1141

Introduction.....	1143
attribute (radsrv-grp).....	1144
authentication.....	1147
client (radsecproxy-srv).....	1148
client mutual-authentication.....	1150
client name-check.....	1151
client trustpoint.....	1152
clear radius local-server statistics.....	1154
copy fdb-radius-users (to file).....	1155
copy local-radius-user-db (from file).....	1157
copy local-radius-user-db (to file).....	1158
crypto pki enroll local (deleted).....	1159
crypto pki enroll local local-radius-all-users (deleted).....	1160
crypto pki enroll local user (deleted).....	1161
crypto pki export local pem (deleted).....	1162
crypto pki export local pkcs12 (deleted).....	1163
crypto pki trustpoint local (deleted).....	1164
debug crypto pki (deleted).....	1165
domain-style.....	1166
egress-vlan-id (radsrv-grp).....	1167
egress-vlan-name (radsrv-grp).....	1168
group (radsrv).....	1169
help radius-attribute.....	1170
nas.....	1172
nas message-authenticator (radsrv).....	1174
radius-secure-proxy local-server.....	1176
radius-server local.....	1177
server auth-port.....	1178
server enable.....	1179
server trustpoint (radsrv).....	1180
show radius local-server group.....	1182
show radius local-server nas.....	1183
show radius local-server statistics.....	1184
show radius local-server trustpoint.....	1186
show radius local-server user.....	1187
user (radsrv).....	1189
vlan (radsrv-grp).....	1192

Chapter 26: Two-factor Authentication (2FA) Commands..... 1193

Introduction.....	1194
2fa allow-reuse.....	1195
2fa create user.....	1196
2fa create user email.....	1198
2fa create user skip-2fa.....	1199
2fa delete user.....	1200

2fa email-expiry-time.....	1201
2fa email-otp.....	1202
2fa email-template.....	1203
2fa export user-data.....	1205
2fa hotp-window-size.....	1206
2fa import user-data source.....	1208
2fa issuer.....	1210
2fa label.....	1212
2fa max-skew.....	1214
2fa radius-email-attribute.....	1216
2fa reject-unconfigured-users.....	1218
2fa reset scratch-codes.....	1219
2fa reset skew.....	1220
2fa skew adjust.....	1221
2fa totp-window-size.....	1223
2fa self-registration port.....	1225
aaa authentication 2fa-registration default group.....	1227
debug 2fa.....	1229
email-attribute (ldap-server).....	1230
service 2fa.....	1231
show 2fa.....	1233
show 2fa email-template.....	1234
show 2fa user.....	1235
show 2fa users.....	1237
show debugging 2fa.....	1238
undebug 2fa.....	1239

Chapter 27: Public Key Infrastructure and Crypto Commands..... 1240

Introduction.....	1241
crypto key generate rsa.....	1242
crypto key zeroize.....	1243
crypto pki authenticate.....	1244
crypto pki enroll.....	1245
crypto pki export pem.....	1246
crypto pki export pkcs12.....	1247
crypto pki import pem.....	1249
crypto pki import pkcs12.....	1251
crypto pki trustpoint.....	1253
crypto verify.....	1255
crypto verify bootrom.....	1257
crypto verify signed.....	1259
enrollment (ca-trustpoint).....	1260
fingerprint (ca-trustpoint).....	1262
lifetime.....	1264
no crypto pki certificate.....	1265
rsa-keypair (ca-trustpoint).....	1266
show crypto key mypubkey rsa.....	1268
show crypto pki certificates.....	1269
show crypto pki trustpoint.....	1271
show hash.....	1273
subject-name (ca-trustpoint).....	1274

Chapter 28: TACACS+ Commands..... 1276

Introduction.....	1277
aaa authorization commands.....	1278

aaa authorization config-commands.....	1280
authorization commands.....	1281
ip tacacs source-interface.....	1283
show tacacs+.....	1285
tacacs-server host.....	1287
tacacs-server key.....	1290
tacacs-server timeout.....	1292

PART 5: Network Management..... 1293

Chapter 29: AMF and AMF Plus Commands..... 1294

Introduction.....	1298
application-proxy ip-filter.....	1299
application-proxy quarantine-vlan.....	1300
application-proxy redirect-url.....	1301
application-proxy threat-protection.....	1302
application-proxy threat-protection send-summary.....	1304
application-proxy whitelist advertised-address.....	1305
application-proxy whitelist enable.....	1306
application-proxy whitelist protection tls.....	1308
application-proxy whitelist server.....	1309
application-proxy whitelist trustpoint (deprecated).....	1311
area-link.....	1312
atmf-arealink.....	1314
atmf-link.....	1316
atmf amfplus-license-only.....	1318
atmf area.....	1320
atmf area password.....	1322
atmf authorize.....	1324
atmf authorize provision.....	1326
atmf backup.....	1328
atmf backup area-masters delete.....	1330
atmf backup area-masters enable.....	1331
atmf backup area-masters now.....	1332
atmf backup area-masters synchronize.....	1333
atmf backup bandwidth.....	1334
atmf backup delete.....	1335
atmf backup enable.....	1336
atmf backup guests delete.....	1337
atmf backup guests enable.....	1338
atmf backup guests now.....	1339
atmf backup guests synchronize.....	1340
atmf backup now.....	1341
atmf backup redundancy enable.....	1343
atmf backup server.....	1344
atmf backup stop.....	1346
atmf backup synchronize.....	1347
atmf cleanup.....	1348
atmf container.....	1349
atmf container login.....	1351
atmf controller.....	1352
atmf distribute firmware.....	1353
atmf domain vlan.....	1355
atmf enable.....	1358
atmf group (membership).....	1359

atmf guest-class.....	1361
atmf log-verbose.....	1363
atmf management subnet.....	1364
atmf management vlan.....	1367
atmf master.....	1370
atmf mtu.....	1371
atmf network-name.....	1372
atmf provision (interface).....	1373
atmf provision node.....	1374
atmf reboot-rolling.....	1376
atmf recover.....	1380
atmf recover guest.....	1382
atmf recover led-off.....	1383
atmf recover over-eth.....	1384
atmf recovery-server.....	1385
atmf remote-login.....	1387
atmf restricted-login.....	1389
atmf retry guest-link.....	1391
atmf secure-mode.....	1392
atmf secure-mode certificate expire.....	1394
atmf secure-mode certificate expiry.....	1395
atmf secure-mode certificate renew.....	1396
atmf secure-mode enable-all.....	1397
atmf select-area.....	1399
atmf topology-gui enable.....	1400
atmf trustpoint.....	1402
atmf virtual-crosslink.....	1404
atmf virtual-link.....	1406
atmf virtual-link description.....	1410
atmf virtual-link protection.....	1411
atmf working-set.....	1413
bridge-group (amf-container).....	1416
clear application-proxy threat-protection.....	1418
clear atmf links.....	1419
clear atmf links virtual.....	1420
clear atmf links statistics.....	1421
clear atmf recovery-file.....	1422
clear atmf secure-mode certificates.....	1423
clear atmf secure-mode statistics.....	1424
clone (amf-provision).....	1425
configure boot config (amf-provision).....	1428
configure boot system (amf-provision).....	1430
copy (amf-provision).....	1432
create (amf-provision).....	1434
debug atmf.....	1437
debug atmf packet.....	1439
delete (amf-provision).....	1442
discovery.....	1444
description (amf-container).....	1446
erase factory-default.....	1447
firmware-url.....	1448
http-enable.....	1450
identity (amf-provision).....	1452
license-cert (amf-provision).....	1455
locate (amf-provision).....	1457
log event-host.....	1459
login-fallback enable.....	1460

modeltype.....	1461
service atmf-application-proxy.....	1462
show application-proxy threat-protection.....	1463
show application-proxy whitelist advertised-address.....	1465
show application-proxy whitelist interface.....	1466
show application-proxy whitelist server.....	1468
show application-proxy whitelist supplicant.....	1469
show atmf.....	1471
show atmf area.....	1475
show atmf area guests.....	1479
show atmf area guests-detail.....	1481
show atmf area nodes.....	1484
show atmf area nodes-detail.....	1486
show atmf area summary.....	1488
show atmf authorization.....	1489
show atmf backup.....	1492
show atmf backup area.....	1497
show atmf backup guest.....	1499
show atmf container.....	1502
show atmf detail.....	1506
show atmf group.....	1509
show atmf group members.....	1511
show atmf guests.....	1513
show atmf guests detail.....	1515
show atmf links.....	1518
show atmf links detail.....	1520
show atmf links guest.....	1528
show atmf links guest detail.....	1530
show atmf links statistics.....	1534
show atmf nodes.....	1537
show atmf provision nodes.....	1539
show atmf recovery-file.....	1541
show atmf secure-mode.....	1542
show atmf secure-mode audit.....	1545
show atmf secure-mode audit link.....	1546
show atmf secure-mode certificates.....	1547
show atmf secure-mode sa.....	1550
show atmf secure-mode statistics.....	1553
show atmf tech.....	1555
show atmf virtual-links.....	1559
show atmf working-set.....	1561
show debugging atmf.....	1562
show debugging atmf packet.....	1563
show running-config atmf.....	1564
state.....	1565
switchport atmf-agentlink.....	1567
switchport atmf-arealink.....	1569
switchport atmf-crosslink.....	1571
switchport atmf-guestlink.....	1573
switchport atmf-link.....	1575
type atmf guest.....	1576
type atmf node.....	1577
undebg atmf.....	1580
username (atmf-guest).....	1581

Chapter 30: STOAT Commands..... 1582

Introduction.....	1583
clear stoat collector session counters.....	1584
description (stoat-dest).....	1585
key (stoat-dest).....	1586
name-check (stoat-dest).....	1587
service stoat.....	1588
show stoat collector.....	1589
show stoat destinations.....	1592
shutdown (stoat-dest).....	1594
stoat collector enable.....	1595
stoat collector expiry-period.....	1596
stoat collector key.....	1597
stoat collector trustpoint.....	1599
stoat destination.....	1600
stoat discovery.....	1602
trustpoint (stoat-dest).....	1603
unique-id.....	1604

Chapter 31: Dynamic Host Configuration Protocol (DHCP) Commands.... 1605

Introduction.....	1607
bootfile.....	1608
clear ip dhcp binding.....	1609
default-router.....	1611
dns-server.....	1612
domain-name.....	1614
host (DHCP).....	1615
ip address dhcp.....	1616
ip dhcp bootp ignore.....	1618
ip dhcp globally-authoritative.....	1619
ip dhcp leasequery enable.....	1620
ip dhcp option.....	1621
ip dhcp pool.....	1624
ip dhcp-client default-route distance.....	1625
ip dhcp-client request vendor-identifying-specific.....	1627
ip dhcp-client vendor-identifying-class.....	1628
ip dhcp-relay agent-option.....	1629
ip dhcp-relay agent-option checking.....	1631
ip dhcp-relay agent-option remote-id.....	1632
ip dhcp-relay information policy.....	1634
ip dhcp-relay maxhops.....	1636
ip dhcp-relay max-message-length.....	1637
ip dhcp-relay server-address.....	1639
ip dhcp-relay short-lease.....	1641
ip dhcp-relay use-client-side-address.....	1642
ip dhcp-relay use-dhcp-relay-ip.....	1644
lease.....	1645
network (DHCP).....	1647
next-server.....	1648
option.....	1649
probe enable.....	1651
probe packets.....	1652
probe timeout.....	1653
probe type.....	1654
range.....	1655
route.....	1656
service dhcp-relay.....	1657

service dhcp-server.....	1658
short-lease-threshold.....	1659
show counter dhcp-client.....	1661
show counter dhcp-relay.....	1663
show counter dhcp-server.....	1668
show dhcp lease.....	1671
show ip dhcp binding.....	1672
show ip dhcp pool.....	1674
show ip dhcp-relay.....	1677
show ip dhcp server statistics.....	1679
show ip dhcp server summary.....	1682
subnet-mask.....	1683
vrf.....	1684

Chapter 32: DHCP for IPv6 (DHCPv6) Commands..... 1686

Introduction.....	1688
address prefix.....	1689
address range.....	1691
clear counter ipv6 dhcp-client.....	1693
clear counter ipv6 dhcp-server.....	1694
clear ipv6 dhcp binding.....	1695
clear ipv6 dhcp client.....	1697
dns-server (DHCPv6).....	1698
domain-name (DHCPv6).....	1700
ip dhcp-relay agent-option.....	1701
ip dhcp-relay agent-option checking.....	1703
ip dhcp-relay agent-option remote-id.....	1704
ip dhcp-relay information policy.....	1706
ip dhcp-relay maxhops.....	1708
ip dhcp-relay max-message-length.....	1709
ip dhcp-relay server-address.....	1711
ip dhcp-relay short-lease-ipv6.....	1713
ipv6 address (DHCPv6 PD).....	1715
ipv6 address dhcp.....	1717
ipv6 dhcp client pd.....	1719
ipv6 dhcp option.....	1721
ipv6 dhcp pool.....	1724
ipv6 dhcp server.....	1726
ipv6 local pool.....	1728
ipv6 nd prefix (DHCPv6).....	1730
link-address.....	1733
option (DHCPv6).....	1735
prefix-delegation pool.....	1738
service dhcp-relay.....	1740
show counter dhcp-relay.....	1741
show counter ipv6 dhcp-client.....	1746
show counter ipv6 dhcp-server.....	1748
show ip dhcp-relay.....	1751
show ipv6 dhcp.....	1753
show ipv6 dhcp binding.....	1754
show ipv6 dhcp interface.....	1758
show ipv6 dhcp pool.....	1760
sntp address.....	1762

Chapter 33: Download Portal Commands..... 1763

Introduction.....	1764
aaa authentication download-portal.....	1765
download-portal.....	1767
download-portal reload.....	1768
enable (download-portal).....	1769
file (download-portal).....	1770
http listen.....	1772
http secure-listen.....	1774
secure-listen (download-portal).....	1776
show download-portal.....	1778
uri (download-portal).....	1779

Chapter 34: NTP Commands..... 1780

Introduction.....	1781
ntp authentication-key.....	1782
ntp broadcastdelay.....	1783
ntp master.....	1784
ntp peer.....	1785
ntp rate-limit.....	1787
ntp restrict.....	1788
ntp server.....	1790
ntp source.....	1792
show ntp associations.....	1794
show ntp counters.....	1797
show ntp counters associations.....	1798
show ntp status.....	1799

Chapter 35: SNMP Commands..... 1800

Introduction.....	1801
alias (interface).....	1802
debug snmp.....	1803
show counter snmp-server.....	1805
show debugging snmp.....	1810
show running-config snmp.....	1811
show snmp-server.....	1812
show snmp-server community.....	1813
show snmp-server group.....	1814
show snmp-server trap.....	1815
show snmp-server user.....	1816
show snmp-server view.....	1817
snmp trap link-status.....	1818
snmp trap link-status suppress.....	1819
snmp-server.....	1821
snmp-server community.....	1823
snmp-server contact.....	1824
snmp-server enable trap.....	1825
snmp-server engineID local.....	1829
snmp-server engineID local reset.....	1831
snmp-server group.....	1832
snmp-server host.....	1834
snmp-server legacy-ifadminstatus.....	1837
snmp-server location.....	1838
snmp-server source-interface.....	1839
snmp-server startup-trap-delay.....	1840
snmp-server system-name.....	1841

snmp-server user.....	1842
snmp-server view.....	1845
snmp-server vrf.....	1846
test snmp trap snmp.....	1847
undebg snmp.....	1848

Chapter 36: LLDP Commands..... 1849

Introduction.....	1850
clear lldp statistics.....	1851
clear lldp table.....	1852
debug lldp.....	1853
lldp faststart-count.....	1855
lldp holdtime-multiplier.....	1856
lldp management-address.....	1857
lldp med-notifications.....	1859
lldp med-tlv-select.....	1860
lldp non-strict-med-tlv-order-check.....	1862
lldp notification-interval.....	1863
lldp notifications.....	1864
lldp port-number-type.....	1865
lldp reinit.....	1867
lldp run.....	1868
lldp timer.....	1869
lldp tlv-select.....	1870
lldp transmit receive.....	1872
lldp tx-delay.....	1874
location civic-location configuration.....	1875
location civic-location identifier.....	1880
location coord-location configuration.....	1881
location coord-location identifier.....	1883
location elin-location.....	1884
show debugging lldp.....	1885
show lldp.....	1887
show lldp interface.....	1890
show lldp local-info.....	1893
show lldp neighbors.....	1898
show lldp neighbors detail.....	1900
show lldp statistics.....	1904
show lldp statistics interface.....	1907
show location.....	1910

Chapter 37: Mail (SMTP) Commands..... 1912

Introduction.....	1913
debug mail.....	1914
delete mail.....	1915
mail.....	1916
mail from.....	1918
mail smtpserver.....	1919
mail smtpserver authentication.....	1920
mail smtpserver port.....	1922
mail smtpserver tls.....	1924
show counter mail.....	1926
show mail.....	1927
undebg mail.....	1928

Chapter 38:	RMON Commands.....	1929
	Introduction.....	1930
	rmon alarm.....	1931
	rmon collection history.....	1936
	rmon collection stats.....	1938
	rmon event.....	1939
	show rmon alarm.....	1940
	show rmon event.....	1941
	show rmon history.....	1942
	show rmon statistics.....	1944
 Chapter 39:	 Secure Shell (SSH) Commands.....	 1945
	Introduction.....	1947
	banner login (SSH).....	1948
	clear ssh.....	1949
	crypto key destroy hostkey.....	1950
	crypto key destroy userkey.....	1951
	crypto key generate hostkey.....	1952
	crypto key generate userkey.....	1954
	crypto key pubkey-chain knownhosts.....	1956
	crypto key pubkey-chain userkey.....	1958
	debug ssh client.....	1960
	debug ssh server.....	1961
	service ssh.....	1962
	show banner login.....	1964
	show crypto key hostkey.....	1965
	show crypto key pubkey-chain knownhosts.....	1967
	show crypto key pubkey-chain userkey.....	1969
	show crypto key userkey.....	1971
	show running-config ssh.....	1973
	show ssh.....	1975
	show ssh client.....	1978
	show ssh server.....	1979
	show ssh server allow-users.....	1982
	show ssh server deny-users.....	1983
	ssh.....	1984
	ssh client.....	1987
	ssh client allow-legacy-ssh-rsa.....	1990
	ssh client vrf.....	1991
	ssh server.....	1992
	ssh server allow-legacy-ssh-rsa.....	1994
	ssh server allow-users.....	1995
	ssh server authentication.....	1997
	ssh server deny-users.....	1999
	ssh server max-auth-tries.....	2001
	ssh server resolve-host.....	2002
	ssh server scp.....	2003
	ssh server secure-algs.....	2004
	ssh server secure-ciphers.....	2005
	ssh server secure-hostkey.....	2006
	ssh server secure-kex.....	2007
	ssh server secure-mac.....	2008
	ssh server sftp.....	2009
	ssh server tcpforwarding.....	2010

ssh server vrf.....	2011
undebg ssh client.....	2012
undebg ssh server.....	2013

Chapter 40: Trigger Commands..... 2014

Introduction.....	2015
active (trigger).....	2016
day.....	2017
debug trigger.....	2019
description (trigger).....	2020
repeat.....	2021
script.....	2023
show debugging trigger.....	2025
show running-config trigger.....	2026
show trigger.....	2027
test.....	2032
time (trigger).....	2033
trap.....	2035
trigger.....	2036
trigger activate.....	2037
type atmf guest.....	2038
type atmf node.....	2039
type cpu.....	2042
type env-sensor.....	2044
type interface.....	2047
type linkmon-probe.....	2048
type log.....	2050
type memory.....	2051
type periodic.....	2052
type ping-poll.....	2053
type reboot.....	2054
type time.....	2055
undebg trigger.....	2056

Chapter 41: Ping-Polling Commands..... 2057

Introduction.....	2058
active (ping-polling).....	2059
clear ping-poll.....	2060
critical-interval.....	2061
debug ping-poll.....	2062
description (ping-polling).....	2063
fail-count.....	2064
ip (ping-polling).....	2066
length (ping-poll data).....	2067
normal-interval.....	2068
ping-poll.....	2069
sample-size.....	2070
show counter ping-poll.....	2072
show ping-poll.....	2075
source-ip.....	2079
timeout (ping polling).....	2081
up-count.....	2082
undebg ping-poll.....	2083

PART 6: Firewall and Network Address Translation (NAT).....2084

Chapter 42:	Firewall Commands.....	2085
	Introduction.....	2086
	clear firewall connections.....	2087
	connection-limit (firewall).....	2088
	connection-log events.....	2090
	debug firewall.....	2091
	firewall.....	2092
	geoip update-interval.....	2093
	ip subnet dynamic geoip.....	2094
	ipv6 subnet dynamic geoip.....	2095
	ip tcp timeout established.....	2096
	move rule (firewall).....	2097
	protect (firewall).....	2098
	rule (firewall).....	2099
	show connection-log events.....	2103
	show firewall.....	2104
	show firewall connections.....	2105
	show firewall connections limits.....	2106
	show firewall connections limits config-check.....	2107
	show firewall rule.....	2108
	show firewall rule config-check.....	2110
	show debugging firewall.....	2111
	show running-config firewall.....	2112
Chapter 43:	Application and Entity Commands.....	2113
	Introduction.....	2114
	application.....	2115
	dport.....	2117
	dscp.....	2119
	host (network).....	2121
	icmp-code.....	2123
	icmp-type.....	2125
	ip address (host).....	2127
	ip subnet.....	2129
	ipv6 address (host).....	2131
	ipv6 subnet.....	2134
	mac-address (host).....	2136
	network (zone).....	2138
	protocol.....	2140
	show application.....	2142
	show application detail.....	2143
	show entity.....	2145
	sport.....	2148
	zone.....	2150
Chapter 44:	NAT Commands.....	2152
	Introduction.....	2153
	enable (nat).....	2154
	ip limited-local-proxy-arp.....	2155
	local-proxy-arp.....	2156
	move rule (nat).....	2157
	nat.....	2158
	rule (nat).....	2159
	show nat.....	2164

	show nat rule.....	2165
	show nat rule config-check.....	2167
	show running-config nat.....	2168
PART 7:	Advanced Network Protection.....	2169
Chapter 45:	IPS Commands.....	2170
	Introduction.....	2171
	alert-thresholding.....	2172
	category action (IPS).....	2173
	ips.....	2174
	protect (IPS).....	2175
	provider (IPS).....	2176
	show ips.....	2177
	show ips categories.....	2178
	show ips categories detail.....	2181
	show running-config ips.....	2183
	sid.....	2184
	update-interval (IPS).....	2185
Chapter 46:	URL Filtering Commands.....	2187
	Introduction.....	2188
	blacklist.....	2189
	log url-requests.....	2190
	protect (url-filter).....	2191
	show running-config url-filter.....	2192
	show url-filter.....	2193
	url-filter reload custom-lists.....	2194
	url-filter.....	2195
	whitelist (url-filter).....	2196
Chapter 47:	Application Awareness Commands.....	2197
	Introduction.....	2198
	counters detailed.....	2199
	dpi.....	2200
	enable (dpi).....	2201
	hostname (application).....	2203
	provider (dpi).....	2204
	show dpi.....	2205
	show dpi statistics.....	2206
	show running-config dpi.....	2208
	web-categorization.....	2209
PART 8:	Virtual Private Networks (VPNs).....	2211
Chapter 48:	IPsec Commands.....	2212
	Introduction.....	2214
	clear isakmp sa.....	2215
	crypto ipsec profile.....	2216
	crypto isakmp key.....	2218
	crypto isakmp peer.....	2222
	crypto isakmp profile.....	2225

debug isakmp.....	2227
dpd-interval.....	2229
dpd-timeout.....	2230
interface tunnel (IPsec).....	2231
lifetime (IPsec Profile).....	2232
lifetime (ISAKMP Profile).....	2233
no debug isakmp.....	2234
pfs.....	2235
rekey.....	2237
show debugging isakmp.....	2239
show interface tunnel (IPsec).....	2240
show ipsec counters.....	2241
show ipsec peer.....	2242
show ipsec policy.....	2244
show ipsec profile.....	2245
show ipsec sa.....	2247
show isakmp counters.....	2248
show isakmp key (IPsec).....	2249
show isakmp peer.....	2250
show isakmp profile.....	2251
show isakmp sa.....	2253
show tunnel inline-processing counters.....	2254
transform (IPsec Profile).....	2257
transform (ISAKMP Profile).....	2259
tunnel destination (IPsec).....	2261
tunnel inline-processing.....	2263
tunnel local name (IPsec).....	2264
tunnel local selector.....	2265
tunnel mode ipsec.....	2267
tunnel oper-status-control.....	2268
tunnel protection ipsec (IPsec).....	2271
tunnel remote name (IPsec).....	2272
tunnel remote selector.....	2273
tunnel security-reprocessing.....	2276
tunnel selector paired.....	2277
tunnel source (IPsec).....	2278
undebg isakmp.....	2280
version (ISAKMP).....	2281

Chapter 49: GRE Tunneling Commands..... 2282

Introduction.....	2283
interface tunnel (GRE).....	2284
show interface tunnel (GRE).....	2285
tunnel checksum.....	2286
tunnel dscp.....	2287
tunnel destination (GRE).....	2288
tunnel local name (GRE).....	2290
tunnel mode gre.....	2291
tunnel protection ipsec (GRE).....	2292
tunnel remote name (GRE).....	2293
tunnel security-reprocessing.....	2294
tunnel source (GRE).....	2295
tunnel ttl.....	2297

Chapter 50: OpenVPN Commands..... 2298

Introduction.....	2299
ip tcp adjust-mss.....	2300
ipv6 tcp adjust-mss.....	2302
show interface tunnel (OpenVPN).....	2304
show openvpn connections.....	2305
show openvpn connections detail.....	2306
tunnel mode openvpn tap.....	2307
tunnel mode openvpn tun.....	2308
tunnel openvpn authentication.....	2309
tunnel openvpn cipher.....	2310
tunnel openvpn expiry-bytes.....	2312
tunnel openvpn expiry-seconds.....	2313
tunnel openvpn port.....	2314
tunnel openvpn route.....	2315
tunnel openvpn tagging.....	2317
tunnel openvpn tls-crypt.....	2318
tunnel openvpn tls-version-min.....	2319
tunnel openvpn verify-client-certificate trustpoint.....	2320
tunnel openvpn verify-client-certificate strict-common-name-check.....	2322
tunnel security-reprocessing.....	2324

Chapter 51: L2TPv3 Ethernet Pseudowire Commands..... 2325

Introduction.....	2326
interface tunnel (L2TPv3).....	2327
l2tp unmanaged port.....	2328
show interface tunnel (L2TPv3).....	2329
tunnel destination (L2TPv3).....	2330
tunnel df.....	2332
tunnel local id.....	2334
tunnel mode l2tp v3.....	2335
tunnel protection ipsec.....	2336
tunnel remote id.....	2337
tunnel security-reprocessing.....	2338
tunnel source (L2TPv3).....	2339

Chapter 52: Transitioning IPv4 to IPv6 Commands..... 2341

Introduction.....	2342
4to6-mapping.....	2343
br-address (software).....	2344
clear 4to6-mapping.....	2345
ip dns forwarding dns46.....	2347
ip dns forwarding dns64.....	2350
limits (4to6-mapping).....	2352
map4to6 (4to6-mapping).....	2353
map6to4 (4to6-mapping).....	2355
mesh-mode.....	2357
method.....	2358
originator (4to6-mapping) (deprecated).....	2359
responder (4to6-mapping) (deprecated).....	2360
rule.....	2361
show 4to6-mapping.....	2363
show ip dns forwarding dns46.....	2364
show running-config software-configuration.....	2365
show software-configuration.....	2366
software-configuration.....	2368

tunnel destination (DS-Lite).....	2369
tunnel mode ds-lite.....	2370
tunnel mode lw4o6.....	2371
tunnel mode map-e.....	2372
tunnel security-reprocessing.....	2373
tunnel software.....	2374
upstream-interface.....	2375

Chapter 53: IPv6 Tunneling Commands.....2376

Introduction.....	2377
interface tunnel (IPv6).....	2378
ip address (IP Addressing and Protocol).....	2379
ip tcp adjust-mss.....	2381
ipv6 address.....	2383
ipv6 tcp adjust-mss.....	2385
mtu.....	2387
show interface tunnel (IPv6).....	2389
tunnel destination (IPv6).....	2390
tunnel dscp.....	2392
tunnel mode (IPv6).....	2393
tunnel source (IPv6).....	2394
tunnel ttl.....	2396

Part 1: Setup and Troubleshooting

1

CLI Navigation Commands

- Contents**
- **Introduction** on page 35
 - **configure terminal** on page 36
 - **disable (Privileged Exec mode)** on page 37
 - **do** on page 38
 - **enable (Privileged Exec mode)** on page 39
 - **end** on page 41
 - **exit** on page 42
 - **help** on page 43
 - **logout** on page 44
 - **show history** on page 45

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.

configure terminal

Overview This command enters the Global Configuration command mode.

Syntax `configure terminal`

Mode Privileged Exec

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

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


disable (Privileged Exec mode)

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

Syntax disable

Mode Privileged Exec

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

```
awplus# disable
awplus>
```

Related commands **enable (Privileged Exec mode)**
end
exit

do

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

Syntax do <command>

Parameter	Description
<command>	Specify the command and its parameters.

Mode Any configuration mode

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

enable (Privileged Exec mode)

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

Syntax `enable [<privilege-level>]`

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

Mode User Exec

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

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

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

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

```
awplus> enable  
awplus#
```

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

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

Related commands

- disable (Privileged Exec mode)**
- enable password**
- enable secret (deprecated)**
- exit**
- service password-encryption**
- username**

end

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

Syntax end

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

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

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

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

```
awplus# configure terminal
awplus(config)# interface 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 The following shows typical output.

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 The following shows typical output.

Example output from the show history command

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

2

Device GUI and Vista Manager EX Commands

- Contents**
- **Introduction** on page 47
 - **atmf topology-gui enable** on page 48
 - **gui preference flash** on page 50
 - **http check-api-content-type-header** on page 51
 - **http client vrf** on page 52
 - **http log webapi-requests** on page 53
 - **http port** on page 54
 - **http secure-port** on page 56
 - **http tls-version-minimum** on page 58
 - **http trustpoint** on page 59
 - **http vrf** on page 61
 - **log event-host** on page 62
 - **service http** on page 63
 - **show http** on page 64
 - **show http client** on page 65
 - **update webgui now** on page 66

Introduction

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

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

atmf topology-gui enable

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

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

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

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

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

Mode Global Configuration mode

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

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

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

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

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

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

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

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

Related **atmf enable**
commands **log event-host**
service http

gui preference flash

Overview Use this command to change the device's preference for which GUI file it uses, if it needs to choose between a GUI file in Flash memory and one downloaded from the Allied Telesis update server.

By default the preference is for a GUI file from the update server. If the device does not have a GUI file from the update server, it will use one from Flash, if present. This command reverses the preference. With this command, the device will use a GUI file from Flash, if present. Otherwise, it will use a file from the update server, if present.

You need to use this command if you want to:

- download a GUI file and save it on the device, or
- use Vista Manager to update the Device GUI.

Use the **no** variant of this command to make the device use a GUI file from the update server by preference.

Syntax gui preference flash
no gui preference flash

Default Disabled.

Mode Global Configuration

Example To allow the device to use a Device GUI file that you have manually downloaded and stored in Flash memory, use the commands:

```
awplus# configure terminal
awplus(config)# gui preference flash
```

Related commands [update webgui now](#)

Command changes Version 5.5.0-2.1: command added

http check-api-content-type-header

Overview Use this command to make sure that all the web-based Device GUI HTTP/S requests coming into the device have the expected Content-Type HTTP header set to 'application/json'. This makes the device's HTTP request processing more secure.

Do not use this command if you use Vista Manager EX. Some of its requests use different header settings, and this command will cause the device to drop those requests.

Use the **no** variant of this command to disable this check.

Syntax http check-api-content-type-header
no http check-api-content-type-header

Default Disabled

Mode Global Configuration

Usage notes We recommend you enable the HTTP header checking, unless you are using Vista Manager EX.

Note that it requires GUI version 2.19.0 or later.

Example To check the validity of device GUI HTTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# http check-api-content-type-header
```

To disable the check again, use the commands:

```
awplus# configure terminal
awplus(config)# no http check-api-content-type-header
```

Related commands
Command changes

[show http](#)

Version 5.5.4-2.1: command added

http client vrf

Overview Use this command to enable the use of a specific VRF for the command `copy http`.

Use the **no** variant of this command to disable the configured VRF.

Syntax `http client vrf <vrf-name>`
`no http client vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when copying a file using HTTP.

Default Global VRF.

Mode Privileged Exec

Examples To enable the use of VRF 'MyVRF', use the commands:

```
awplus# configure terminal
awplus(config)# http client vrf MyVRF
```

To remove a specified VRF and revert to the global VRF, use the commands:

```
awplus# configure terminal
awplus(config)# no http client vrf
```

Output The following shows typical output.

Example output if the specified VRF does not exist:

```
"Invalid VRF instance MyVRF"
```

Related commands [copy \(filename\)](#)
[show http client](#)

Command changes Version 5.5.2-1.1: command added

http log webapi-requests

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

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

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

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

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

Default Web API request logging is disabled.

Mode Global Configuration

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

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

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

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

Related commands [http port](#)
[service http](#)
[show log](#)

Command changes Version 5.4.8-1.1: command added

http port

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

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

Syntax http port {<1-65535>|none}

no http port

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

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

Mode Global Configuration

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

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

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

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

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

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

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

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

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

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

http secure-port

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

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

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

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

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

Mode Global Configuration

Usage notes Do not configure the HTTPS port to be the same as the HTTP port.
Note that if you are using Vista Manager EX and need to change the HTTPS port, you must use certificate-based authorization in Vista Manager EX. See the [Vista Manager EX Installation Guide](#) for instructions.

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

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

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

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

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

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

Related commands [http port](#)
[service http](#)
[show http](#)

Command changes Version 5.4.7-1.1: command added on AR-Series devices
Version 5.4.7-2.4: **none** parameter added
Version 5.4.8-0.2: command added on AlliedWare Plus switches

http tls-version-minimum

Overview Use this command to set the minimum TLS version the device will use for all HTTP services running on the device. This includes the web-based GUI and RESTCONF.

Use the **no** variant of this command to return to the default minimum TLS version.

Syntax `http tls-version-minimum {1.2|1.3}`
`no http tls-version-minimum`

Parameter	Description
1.2	Use a minimum of TLS 1.2.
1.3	Use a minimum of TLS 1.3.

Default 1.2

Mode Global Configuration

Example To use a minimum of TLS 1.3, use the commands:

```
awplus# configure terminal
awplus(config)# http tls-version-minimum 1.3
```

To return to using a minimum of TLS 1.2, use the commands:

```
awplus# configure terminal
awplus(config)# no http tls-version-minimum
```

Related commands [show http](#)

Command changes Version 5.5.5-1.1: command added

http trustpoint

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

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

Syntax http trustpoint <trustpoint-name>
no http trustpoint

Parameter	Description
<trustpoint-name>	Name of trustpoint

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

Mode Global Configuration

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

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

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

Create the root and server certificates for this trustpoint:

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

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

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

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

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

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

Related commands

- crypto pki trustpoint**
- show crypto pki certificates**
- show crypto pki trustpoint**

Command changes Version 5.5.1-2.1: command added

http vrf

Overview Use this command to configure an HTTP server to be run within a specified VRF.

Use the **no** variant of this command to remove a VRF configuration from the HTTP server.

Syntax `http vrf <vrf-name>`

`no http vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when running the HTTP server. The name of the VRF instance.

Default By default the HTTP server uses the global VRF.

Mode Global Configuration

Examples To configure VRF 'MyVRF', use the commands:

```
awplus# configure terminal
awplus(config)# http vrf MyVRF
```

To return the HTTP server to the global VRF, use the commands:

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

Related commands [service http](#)
[show http](#)

Command changes Version 5.5.2-1.1: command added

log event-host

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

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

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

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

Default Log events are disabled by default.

Mode Global Configuration

Usage notes Event hosts are set so syslog sends the messages out as they come.
Note that there is a difference between log event and log host messages:

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

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

```
Node1# configure terminal
```

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

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

```
Node1# configure terminal
```

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

Related commands [atmf topology-gui enable](#)

service http

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

This service is required to support Vista Manager EX™ 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 Device 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 The following shows typical output.

Example output from the show http command

```
awplus#show http
HTTP Server Configuration

-----
HTTP server                : Enabled
Listen Addresses :
Secure                   : *:443
HTTP                    : *:80
Check API Content-Type Header : Disabled
TLS version minimum      : 1.2

Web GUI Information
-----
GUI file in use           : awplus-gui_555_41.gui

Server Certificate
-----

Subject      : O = Allied-Telesis, CN = AlliedwarePlusDefault, serialNumber =
<number>
Issuer       : O = "Allied Telesis, Inc.", CN = AlliedWarePlusCA, serialNumber =
<number>
Valid From   : Mar 15 14:09:40 2023 GMT
Valid To     : Mar  2 14:09:40 2073 GMT
Fingerprints :

SHA-1       : 8F:...EE
SHA-256     : 4F:...FF
```

Related commands [clear line vty](#)
[http check-api-content-type-header](#)
[http tls-version-minimum](#)
[service http](#)

show http client

Overview Use this command to show the current HTTP client VRF.

Syntax show http client

Mode Privileged Exec

Usage notes If no VRF has been set, the show command shows 'None'.

Example To display the HTTP client VRF, use the commands:

```
awplus# show http client
```

Output The following shows typical output.

Example output from show http client

```
awplus#show http client
Hyper-Text Transfer Protocol Client Configuration
-----
VRF                                     : MyVRFPoE
```

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

Command changes Version 5.5.2-1.1: command added

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

Examples To check for GUI updates, use the following command:
awplus# update webgui now

Related commands [gui preference flash](#)
[show resource](#)

Command changes Version 5.4.9-2.1: command added to SBx908 GEN2

3

File and Configuration Management Commands

- Contents**
- **Introduction** on page 69
 - **boot config-file** on page 71
 - **boot config-file backup** on page 72
 - **boot system** on page 73
 - **boot system backup** on page 74
 - **cd** on page 75
 - **copy (filename)** on page 76
 - **copy debug** on page 78
 - **copy running-config** on page 79
 - **copy startup-config** on page 80
 - **copy zmodem** on page 81
 - **crypto verify** on page 82
 - **crypto verify bootrom** on page 84
 - **crypto verify signed** on page 86
 - **delete** on page 87
 - **delete debug** on page 88
 - **dir** on page 89
 - **edit** on page 91
 - **erase factory-default** on page 93
 - **erase startup-config** on page 94
 - **ip tftp source-interface** on page 95
 - **ip tftp vrf** on page 96
 - **ipv6 tftp source-interface** on page 97
 - **mkdir** on page 98
 - **move** on page 99
 - **move debug** on page 100
 - **pwd** on page 101
 - **rmdir** on page 102
 - **show boot** on page 103
 - **show hash** on page 105
 - **show file** on page 106
 - **show file systems** on page 107
 - **show running-config** on page 110
 - **show running-config interface** on page 114
 - **show running-config unencrypted** on page 117
 - **show startup-config** on page 118
 - **show version** on page 119

- **strict-user-process-control** on page 120
- **strict-user-process-control force** on page 121
- **write file** on page 122
- **write memory** on page 123
- **write terminal** on page 124

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

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

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

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

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

Syntax for directory listings A leading slash (/) indicates the root of the current file system location. In commands where you need to specify the local file system's flash base directory, you may use **flash** or **flash:** or **flash:/**. For example, these commands are all the same:

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

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

boot config-file

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

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

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

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

Mode Global Configuration

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

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

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

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

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

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

boot config-file backup

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

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

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

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

Mode Global Configuration

Usage notes For an 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. You can also use the boot menu to select a release file source. To access the boot menu, type Ctrl-B at bootup.

Syntax boot system <filepath-filename>
no boot system

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

Mode Global Configuration

Usage notes This switch stores release files in flash memory.

Examples To boot up with the release file TQ7403R-5.5.5-2.1.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:/TQ7403R-5.5.5-2.1.rel
```

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

boot system backup

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

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

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

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

Mode Global Configuration

Examples To specify the file TQ67403R-5.5.5-1.1.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# boot system backup flash:/TQ67403R-5.5.5-1.1.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><directory-name></code>	Name and path of the directory.

Mode Privileged Exec

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

```
awplus# cd images
```

Related commands

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

copy (filename)

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

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

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

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

Mode Privileged Exec

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

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

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

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

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

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

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

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

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

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


Related
commands

- copy zmodem**
- copy buffered-log**
- copy permanent-log**
- show file systems**

copy debug

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

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

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

Mode Privileged Exec

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

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

Output The following shows typical output.

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><source-name></code>	The filename and path of a configuration file. This must be a valid configuration file with a .cfg filename extension. Specify this when you want the script in the file to become the new running-config. See Introduction for valid syntax.
<code><destination-name></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 Introduction 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
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a .cfg filename extension. Specify this to copy the script in the file into the startup-config file. Note that this does not make the copied file the new startup file, so any further changes made in the configuration file are not added to the startup-config file unless you reuse this command. See Introduction for valid syntax.
<destination-name>	The destination and filename that you are saving the startup-config as. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction for valid syntax.

Mode Privileged Exec

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

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

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

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

Related commands [copy running-config](#)

copy zmodem

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

Syntax copy <source-name> zmodem
copy zmodem

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction 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](#)

crypto verify

Overview Use this command to compare the SHA256 checksum of a file with its correct checksum. This confirms that the file has not been corrupted or interfered with during download. You can verify any kind of file, but you cannot specify a file path, so the file must be stored in the top level of the device's flash memory.



CAUTION: *If a file fails to verify and you believe the file may have been interfered with, we recommend immediately performing a security audit of your network.*

Once the device has verified the file, you can use the **copy running-config startup-config** command to save the file/hash pair in the running configuration. If you do this, the device will verify the file every time it boots up and will take action if the verification fails.

The action taken when verification fails on boot-up depends on the type of file:

- If the boot-up firmware file fails verification, the device will display the following warning message after booting: "% Verification Failed". If this occurs because the saved hash is incorrect, use this command to replace the hash. If this occurs because the firmware file is corrupted or may have been interfered with, ensure that your device is secure, then replace the failed file with a known good file and reboot.
- If you use the **gui** parameter and the GUI fails verification, the device will boot up but the GUI will be disabled (the **service http** command will be disabled).
- If any other file fails verification, the device will display the following warning message after booting: "% Verification Failed"

You can use the **show hash** command to see the current hash of a file.

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

Syntax `crypto verify <filename> <hash-value>`
`crypto verify gui <hash-value>`
`no crypto verify <filename>`

Parameter	Description
<code><filename></code>	The AlliedWare Plus file that you want to verify
<code>gui</code>	Verify the current Device GUI file
<code><hash-value></code>	The known correct checksum of the file. For firmware and GUI files, the correct checksum is listed in the sha256sum file that is available from the Allied Telesis Download Center.

Default	No default
Mode	Global Configuration
Usage notes	All models of a particular series run the same firmware file and therefore have the same checksum for that firmware file. For example, all x930 Series switches have the same checksum. If your network has extremely strict security requirements, such as FIPS compliance, you may need to verify the bootloader on boot-up and use signature verification for the firmware file. To configure these, use the commands crypto verify bootrom and crypto verify signed. These commands make it difficult to upgrade the bootloader or firmware, so only use them if necessary.
Examples	To verify the firmware file for 5.5.3-0.1 on an x930 Series switch, use the commands: <pre>awplus# configure terminal awplus(config)# crypto verify x930-5.5.3-0.1.rel 7f22d8a30c991a4ddc0a2aed47246282b23b4e4a865e07f79795c0959c47de78</pre>
Related commands	crypto verify bootrom crypto verify signed show hash
Command changes	Version 5.5.5-1.1: command available on all AlliedWare Plus devices Version 5.5.3-0.1: gui parameter added; <filename> parameter expanded to cover all file types

crypto verify bootrom

Overview Use this command to compare the SHA256 checksum hash value of a bootloader with its correct checksum. This confirms that the bootloader has not been corrupted or interfered with.

If the verification fails, contact Allied Telesis customer support.

You can use the **write** command to save the hash value to the boot configuration file. The device will verify the checksum every time it boots up and will warn you if it fails the verification.

You can use the **no** variant of this command to remove the bootrom/hash combination from the running configuration.

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

Parameter	Description
<code><hash-value></code>	The known correct checksum of the bootloader. To see the correct hash value, run the command show hash bootrom straight after you first boot the device up, or check the Deployment Guide for the device.

Default No default

Mode Global Configuration

Usage notes Please use this command in accordance with the User Guidance documentation for your required security certification.

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

Examples To verify the bootrom file, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify bootrom
5e80e70b6a2200965abf5f62f72af1bdc1654f3726bdff554afcbd76270c91
```

Note that the hash in this example is an example only; it is not the hash of the device's bootloader.

Related commands [crypto verify](#)
[crypto verify signed](#)
[show hash](#)

Command changes Version 5.5.5-1.1: command available on all AlliedWare Plus devices

crypto verify signed

Overview Use this command to compare the HMAC-SHA checksum hash value of a firmware file with its correct checksum. This confirms that the firmware has not been corrupted or interfered with.

Please use this command in accordance with the User Guidance documentation for your required security certification.

If the verification fails, contact Allied Telesis customer support.

Syntax `crypto verify signed <filename> <hash-value>`

Parameter	Description
<code><filename></code>	The AlliedWare Plus file that you want to verify
<code><hash-value></code>	The known correct checksum of the file. This is a keyed HMAC-SHA hash. This is available in a .sig file, which you can get from your Allied Telesis customer representative.

Default No default

Mode Global Configuration

Usage notes You can use the `write` command to save the hash value to the boot configuration file. The device will verify the checksum every time it boots up and will warn you if it fails the verification.

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

Examples To use signature verification to verify the firmware file for 5.5.3-0.1 on an x930 Series switch, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify signed x930-5.5.3-0.1.rel
3f50420644aebd277dd48b3aee30639801348896fffce231fc5615995ecde5d9
```

Related commands [crypto verify](#)
[crypto verify bootrom](#)
[show hash](#)

Command changes Version 5.5.5-1.1: command available on all AlliedWare Plus devices

delete

Overview This command deletes files or directories.

Syntax delete [force] [recursive] <filename>

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

Mode Privileged Exec

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

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

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

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

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

```
awplus# delete recursive old_configs
```

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

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

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

delete debug

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

Syntax delete debug <source-name>

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

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

Output The following shows typical output.

CLI prompt after entering the delete debug command

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

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

dir

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

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

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

Mode Privileged Exec

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

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

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

```
awplus# dir sort name
```

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

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

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

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

Output The following shows typical output.

Example output from the dir command

```
awplus#dir
 630 -rw- Nov 25 2022 23:36:31 example.cfg
23652123 -rw- Nov 25 2022 03:41:18 TQ7403R-5.5.5-2.1.rel
 149 -rw- Nov 25 2022 00:40:35 exception.log
```

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

edit

- Overview** This command opens a text file in the AlliedWare Plus™ text editor. Once opened you can use the editor to alter to the file.
- If you specify a filename and the file already exists, then the editor opens it in the text editor.
- If you do not enter a filename, the editor opens an empty file and prompts you for a name when you exit the editor.
- For information about using the editor, including control sequences, see the [File Management Feature Overview and Configuration Guide](#).

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

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

Mode Privileged Exec

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

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

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

```
awplus# edit
```

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

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

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

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

Related **copy (filename)**
commands **dir**
mkdir
show file

erase factory-default

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

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

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

Syntax erase factory-default

Mode Privileged Exec

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

Note that you cannot use this command if you have **strict-user-process-control** enabled. Disable it before entering the **erase factory-default** command.

Example To erase data, use the command:

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

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

Related commands **atmf cleanup**

erase startup-config

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

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

Syntax erase startup-config

Mode Privileged Exec

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

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

Related commands

- boot config-file backup**
- copy running-config**
- copy startup-config**
- show boot**

ip tftp source-interface

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

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

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

Parameter	Description
<interface>	The 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 PPP or Eth interface).
<ip-add>	The IP address that TFTP requests originate from, in dotted decimal format.

Default There is no default source specified.

Mode Global Configuration

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

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

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

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

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

ip tftp vrf

Overview Use this command to specify a VRF to use when copying a file via TFTP.

Use the **no** variant of this command to remove the VRF from the configuration and set it back to the default VRF.

Syntax `ip tftp vrf <vrf-name>`
`no ip tftp vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when copying a file using TFTP.

Default Global VRF

Mode Global Configuration

Example To configure a VRF called 'red' to use when copying a file via TFTP, use the commands:

```
awplus# configure terminal
awplus(config)# ip tftp vrf red
```

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

Command changes Version 5.5.2-1.1: command added

ipv6 tftp source-interface

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

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

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

Parameter	Description
<interface>	The 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 PPP or Eth interface).
<ipv6-add>	The IPv6 address that TFTP requests originate from, in the format x:x::x:x, for example, 2001:db8::8a2e:7334.

Default There is no default source specified.

Mode Global Configuration

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

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

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

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

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

mkdir

Overview This command makes a new directory.

Syntax `mkdir <name>`

Parameter	Description
<code><name></code>	The name and path of the directory that you are creating.

Mode Privileged Exec

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

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

```
awplus# mkdir images
```

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

move

Overview This command renames or moves a file.

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

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

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

Mode Privileged Exec

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

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

Output 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**

rmkdir

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

Syntax `rmkdir [force] <name>`

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

Mode Privileged Exec

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

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

```
awplus# rmkdir 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# rmkdir force level1
```

Related commands

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

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 The following shows typical output.

Example output from show boot

```
awplus#show boot
Boot configuration
-----
Current software   : TQ7403R-5.5.5-2.1.rel
Current boot image : flash:/TQ7403R-5.5.5-2.1.rel
Backup boot image  : flash:/TQ67403R-5.5.5-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/my.cfg (file exists)
Backup boot config: flash:/backup.cfg (file not found)
Autoboot status    : disabled
```

Parameters in the output from show boot

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

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

show hash

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

Syntax show hash <filename>

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

Mode Privileged Exec

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

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

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

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

Output The following shows typical output.

Example output from show hash

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

Command changes Version 5.5.3-0.1: command added

show file

Overview This command displays the contents of a specified file.

Syntax show file <filename>

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

Mode Privileged Exec

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

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

Related commands [edit](#)
[show file systems](#)

show file systems

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

Syntax show file systems

Mode Privileged Exec

Examples To display the file systems, use the command:
awplus# show file systems

Output The following shows typical output.

```
awplus#show file systems
```

Size(b)	Free(b)	Type	Flags	Prefixes	S/D/V	Lcl/Ntwk	Avail
676.8M	513.6M	flash	rw	flash:	static	local	Y
-	-	system	rw	system:	virtual	local	-
10.0M	9.3M	debug	rw	debug:	static	local	Y
-	-	fserver	rw	fserver:	dynamic	network	N
-	-	tftp	rw	tftp:	-	network	-
-	-	scp	rw	scp:	-	network	-
-	-	sftp	ro	sftp:	-	network	-
-	-	http	ro	http:	-	network	-
-	-	rsync	rw	rsync:	-	network	-

Parameters in the output of the show file systems command

Parameter	Description
Size (b)	The total memory available to this file system. The units are given after the value and are M for Megabytes or K for kilobytes.
Free (b)	The total memory free within this file system. The units are given after the value and are M for Megabytes or K for kilobytes.
Type	The memory type used for this file system, such as: flash system tftp scp sftp http.
Flags	The file setting options: rw (read write), ro (read only).
Prefixes	The prefixes used when entering commands to access the file systems, such as: flash system tftp scp sftp http.
S/D/V	The memory type: Static, Dynamic, Virtual.
Lcl / Ntwk	Whether the memory is located locally or via a network connection.

Parameter	Description
Avail	Whether the memory is accessible: Y (yes), N (no), - (not applicable)

Related [edit](#)
commands [show file](#)

show running-config

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

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

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

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

Parameter	Description																																																		
full	Display the running-config for all features. This is the default setting, so it is the same as entering show running-config .																																																		
<feature>	Display only the configuration for a single feature. The features available depend on your device and will be some of the following list: <table> <tr> <td>access-list</td><td>ACL configuration</td></tr> <tr> <td>antivirus</td><td>Antivirus configuration</td></tr> <tr> <td>application</td><td>Application configuration</td></tr> <tr> <td>as-path</td><td>Autonomous system path filter configuration</td></tr> <tr> <td>as-path access-list</td><td>Configuration of ACLs for AS path filtering</td></tr> <tr> <td>atmf</td><td>Allied Telesis Management Framework configuration</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP) configuration</td></tr> <tr> <td>community-list</td><td>Community-list configuration</td></tr> <tr> <td>crypto</td><td>Security-specific configuration</td></tr> <tr> <td>dhcp</td><td>DHCP configuration</td></tr> <tr> <td>dpi</td><td>Deep Packet Inspection configuration</td></tr> <tr> <td>entity</td><td>Entity configuration</td></tr> <tr> <td>firewall</td><td>Firewall configuration</td></tr> <tr> <td>interface</td><td>Interface configuration. See show running-config interface for further options.</td></tr> <tr> <td>ip</td><td>Internet Protocol (IP) configuration</td></tr> <tr> <td>ip pim dense-mode</td><td>PIM-DM configuration</td></tr> <tr> <td>ip pim sparse-mode</td><td>PIM-SM configuration</td></tr> <tr> <td>ip route</td><td>IP static route configuration</td></tr> <tr> <td>ip-reputation</td><td>IP Reputation configuration</td></tr> <tr> <td>ips</td><td>IPS configuration</td></tr> <tr> <td>ipsec</td><td>Internet Protocol Security (IPsec) configuration</td></tr> <tr> <td>ipv6</td><td>Internet Protocol version 6 (IPv6) configuration</td></tr> <tr> <td>ipv6 access-list</td><td>IPv6 ACL configuration</td></tr> <tr> <td>ipv6 mroute</td><td>IPv6 multicast route configuration</td></tr> <tr> <td>ipv6 prefix-list</td><td>IPv6 prefix list configuration</td></tr> </table>	access-list	ACL configuration	antivirus	Antivirus configuration	application	Application configuration	as-path	Autonomous system path filter configuration	as-path access-list	Configuration of ACLs for AS path filtering	atmf	Allied Telesis Management Framework configuration	bgp	Border Gateway Protocol (BGP) configuration	community-list	Community-list configuration	crypto	Security-specific configuration	dhcp	DHCP configuration	dpi	Deep Packet Inspection configuration	entity	Entity configuration	firewall	Firewall configuration	interface	Interface configuration. See show running-config interface for further options.	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
access-list	ACL configuration																																																		
antivirus	Antivirus configuration																																																		
application	Application configuration																																																		
as-path	Autonomous system path filter configuration																																																		
as-path access-list	Configuration of ACLs for AS path filtering																																																		
atmf	Allied Telesis Management Framework configuration																																																		
bgp	Border Gateway Protocol (BGP) configuration																																																		
community-list	Community-list configuration																																																		
crypto	Security-specific configuration																																																		
dhcp	DHCP configuration																																																		
dpi	Deep Packet Inspection configuration																																																		
entity	Entity configuration																																																		
firewall	Firewall configuration																																																		
interface	Interface configuration. See show running-config interface for further options.																																																		
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																																																		

Parameter	Description
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
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 The following shows typical output.

Example output from show running-config

```
awplus#show running-config
!
service password-encryption
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$Jw0JGPr7YqoExA0GVasdE0
!
service ssh
!
no service telnet
!
service http
!
no clock timezone

...

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

Related commands

- [copy running-config](#)
- [show running-config interface](#)
- [show running-config unencrypted](#)

show running-config interface

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

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

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

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. The specified interfaces must exist.
cfm	Displays running configuration for CFM (Connectivity Fault Management) for the specified interfaces.
dot1x	Displays running configuration for 802.1X port authentication for the specified interfaces.
lacp	Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.
ip igmp	Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.
ip multicast	Displays running configuration for general multicast settings for the specified interfaces.
ip pim sparse-mode	Displays running configuration for PIM-SM (Protocol Independent Multicast - Sparse Mode) for the specified interfaces.
ip pim dense-mode	Displays running configuration for PIM-DM (Protocol Independent Multicasting - Dense Mode) for the specified interfaces.

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

Mode Privileged Exec and Global Configuration

Default Displays information for all protocols on all interfaces

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

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

Output The following shows typical output.

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
!
```

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

show running-config unencrypted

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

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

Syntax show running-config unencrypted

Mode Privileged Exec

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

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

Related commands [show running-config](#)

Command changes Version 5.5.3-2.1: command added

show startup-config

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

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

Syntax show startup-config

Mode Privileged Exec

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

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

Output The following shows typical output.

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$Jw0JGPr7YqoExA0GVasdE0
!
service ssh
!
no service telnet
!
service http
!
no clock timezone

...

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

Related commands

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

show version

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

Syntax show version

Mode User Exec and Privileged Exec

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

```
awplus# show version
```

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

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

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

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

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

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

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands [show running-config](#)
[strict-user-process-control force](#)

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

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

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

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



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

Syntax `strict-user-process-control force`

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands [show running-config](#)
[strict-user-process-control](#)

Command changes Version 5.5.4-1.8: command added

write file

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

Syntax write [file]

Mode Privileged Exec

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

```
awplus# write file
```

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

write memory

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

Syntax write [memory]

Mode Privileged Exec

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

```
awplus# write memory
```

Related commands **copy running-config**
write file
show running-config

write terminal

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

Syntax write terminal

Mode Privileged Exec

Example To display the current configuration of your device, use the command:
awplus# write terminal

Related commands **show running-config**

4

User Access Commands

- Contents**
- **Introduction** on page 127
 - **aaa authentication enable default local** on page 128
 - **aaa local authentication attempts lockout-time** on page 129
 - **aaa local authentication attempts max-fail** on page 130
 - **aaa login fail-delay** on page 132
 - **clear aaa local user lockout** on page 133
 - **clear line console** on page 134
 - **clear line vty** on page 135
 - **enable password** on page 136
 - **enable secret (deprecated)** on page 138
 - **exec-timeout** on page 139
 - **flowcontrol hardware (asyn/console)** on page 141
 - **length (asyn)** on page 143
 - **line** on page 145
 - **privilege level** on page 147
 - **security-password history** on page 148
 - **security-password forced-change** on page 149
 - **security-password lifetime** on page 150
 - **security-password min-lifetime-enforce** on page 151
 - **security-password minimum-categories** on page 153
 - **security-password minimum-length** on page 155
 - **security-password reject-expired-pwd** on page 156
 - **security-password warning** on page 158
 - **service advanced-vty** on page 159
 - **service password-encryption** on page 160
 - **service telnet** on page 161
 - **show aaa local user locked** on page 162
 - **show privilege** on page 164
 - **show security-password configuration** on page 165
 - **show security-password user** on page 166
 - **show telnet** on page 167
 - **show users** on page 168
 - **strict-user-process-control** on page 169
 - **strict-user-process-control force** on page 170
 - **telnet server** on page 171
 - **terminal length** on page 172
 - **terminal resize** on page 173

- **username** on page 174

Introduction

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

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 (deprecated)**

aaa local authentication attempts lockout-time

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

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

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

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

Mode Global Configuration

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

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

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

```
awplus# configure terminal
```

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

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

```
awplus# configure terminal
```

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

Related commands **aaa local authentication attempts max-fail**
aaa local authentication attempts max-fail remote-login-only
clear aaa local user lockout

aaa local authentication attempts max-fail

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

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

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related commands **aaa local authentication attempts logout-time**
aaa local authentication attempts max-fail remote-login-only
clear aaa local user logout

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 logout

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

Syntax clear aaa local user logout {username <username>|all}

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

Mode Privileged Exec

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

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

To unlock all user accounts use the following command:

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

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

clear line console

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

Syntax clear line console 0

Mode Privileged Exec

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

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

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

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

clear line vty

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

Syntax clear line vty <0-32>

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

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

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

Related commands

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

enable password

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

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

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

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

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

Default Level 15

Mode Global Configuration

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

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

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

Related commands

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

enable secret (deprecated)

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

exec-timeout

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

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

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

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

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

Mode Line Configuration

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

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

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

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

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
```

Related commands **line**
service telnet
show running-config

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 commands:

```
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 commands:

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

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

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

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

line

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

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

Parameter	Description
<first-line>	<0-32> Specify the first line number.
<last-line>	<0-32> Specify the last line number.
console	The console terminal line(s) for local access.
vty	Virtual terminal for remote console access.

Mode Global Configuration

Usage notes This command puts you into Line Configuration mode. Once in Line Configuration mode, you can configure console and virtual terminal settings, including setting **speed (asyn)**, **length (asyn)**, 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 no security-password history command. If the history functionality is disabled, all users' password history is reset and all password history is lost.

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

Mode Global Configuration

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

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

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

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

Related commands

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

security-password forced-change

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

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

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

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

Default The forced-change feature is disabled by default.

Mode Global Configuration

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

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

Related commands

- security-password history**
- security-password lifetime**
- security-password min-lifetime-enforce**
- security-password minimum-categories**
- security-password minimum-length**
- security-password reject-expired-pwd**
- security-password warning**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

security-password lifetime

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

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

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

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

Parameter	Description
<0-1000>	Password lifetime specified in days. A value of 0 will disable lifetime functionality and the password will never expire. This is equivalent to the no security-password lifetime command.

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

Mode Global Configuration

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

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

Related commands

- security-password forced-change**
- security-password history**
- security-password min-lifetime-enforce**
- security-password minimum-categories**
- security-password minimum-length**
- security-password reject-expired-pwd**
- security-password warning**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

security-password min-lifetime-enforce

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

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

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

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

Default By default, no minimum lifetime is enforced.

Mode Global Configuration

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

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

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

Related commands

- security-password forced-change**
- security-password history**
- security-password lifetime**
- security-password minimum-categories**
- security-password minimum-length**
- security-password reject-expired-pwd**
- security-password warning**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

Command changes Version 5.4.7-0.2: command added

security-password minimum-categories

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

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

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

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

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

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

Mode Global Configuration

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

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

Related commands

- security-password forced-change**
- security-password history**
- security-password lifetime**
- security-password min-lifetime-enforce**
- security-password minimum-length**
- security-password reject-expired-pwd**
- security-password warning**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

security-password minimum-length

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

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

Parameter	Description
<1-23>	Minimum password length in the range from 1 to 23.

Default The default minimum password length is 1.

Mode Global Configuration

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

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

Related commands

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

security-password reject-expired-pwd

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



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

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

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

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

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

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

Mode Global Configuration

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

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


Related commands

- security-password forced-change**
- security-password history**
- security-password lifetime**
- security-password min-lifetime-enforce**
- security-password minimum-categories**
- security-password minimum-length**
- security-password warning**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

security-password warning

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

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

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

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

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

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

Mode Global Configuration

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

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

Related commands

- security-password forced-change**
- security-password history**
- security-password lifetime**
- security-password min-lifetime-enforce**
- security-password minimum-categories**
- security-password minimum-length**
- security-password reject-expired-pwd**
- show running-config security-password**
- show security-password configuration**
- show security-password user**

service advanced-vty

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

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

Syntax service advanced-vty
no service advanced-vty

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

Mode Global Configuration

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

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

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

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

service password-encryption

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

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

Syntax service password-encryption
no service password-encryption

Mode Global Configuration

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

Validation show running-config
Commands

Related enable password
commands

service telnet

Overview Use this command to enable the telnet server. The server is disabled 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 disabled 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](#)

Command changes Version 5.5.5-2.1: Disabled by default

show aaa local user locked

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

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

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

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

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

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

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

In the Valid column:

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

Syntax show aaa local user locked

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

Example output from the show aaa local user locked command

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

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

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

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

show privilege

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

Syntax show privilege

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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

Parameters in the output of the show users command

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

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

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

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

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

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

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands [show running-config](#)
[strict-user-process-control force](#)

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

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

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

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



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

Syntax `strict-user-process-control force`

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands [show running-config](#)
[strict-user-process-control](#)

Command changes Version 5.5.4-1.8: command added

telnet 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)**.

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

Parameter	Description
<length>	<0-512> Number of rows that the device will display on the currently-active terminal before pausing.

Mode User Exec and Privileged Exec

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

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

Related commands **terminal resize**
length (asyn)

terminal resize

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

Syntax `terminal resize`

Mode User Exec and Privileged Exec

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

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

```
awplus# terminal resize
```

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

username

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

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

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

Parameter	Description		
<name>	The login name for the user. The user name can contain alphanumeric ASCII characters, plus signs (ASCII 43), dashes (ASCII 45), dots (ASCII 46), @ signs (ASCII 64), slashes (ASCII 47), backslashes (ASCII 92), and underscores (ASCII 95). It cannot contain spaces. It must not start with a digit, a plus sign, a dash or an @ sign. It must not end with an @ sign. On the AlliedWare Plus CLI, it is case sensitive. It cannot contain question marks (?), spaces (), or single or double quote characters.		
privilege	The user's privilege level. Use the privilege levels to set the access rights for each user. <table> <tr> <td><1-15></td><td> A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec. </td></tr> </table>	<1-15>	A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.
<1-15>	A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.		
password	A password that the user must enter when logging in. <table> <tr> <td>8</td><td> The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. </td></tr> </table>	8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form.
8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form.		

Parameter	Description
	Note that the user needs to enter the plain-text version of the password when logging in.
<code><password></code>	The user's password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: • uppercase letters: A to Z • lowercase letters: a to z • digits: 0 to 9 • special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.

Mode Global Configuration

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

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

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

```
awplus# configure terminal
```

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

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

```
awplus# configure terminal
```

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

Related commands **enable password**
security-password minimum-categories
security-password minimum-length

5

Update Manager Commands

- Contents**
- **Introduction** on page 179
 - **show resource** on page 180
 - **update now** on page 181
 - **update webgui now** on page 182

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](#).

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
<resource-name>	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 The following shows typical output.

Example output for show resource

awplus#show resource				
Resource Name	Status	Version	Interval	Last Download Next Download Check
iprep_et_rules	Checking	1.1	4 hours	Wed Dec 31 23:59:00 2020 Thu Jan 1 01:00:00 2020

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 now](#)
[update webgui now](#)

Command changes Version 5.4.9-2.1: command added to SBx908 GEN2

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><resource-name></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 a 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 do an update check and update all available resources, use the following command:

```
awplus# update all now
```

To do an update check and update the device's GUI, use the following command:

```
awplus# update webgui now
```

Related commands [show resource](#)
[update webgui now](#)

Command changes Version 5.4.9-2.1: command added to SBx908 GEN2

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

Examples To check for GUI updates, use the following command:
awplus# update webgui now

Related commands [gui preference flash](#)
[show resource](#)

Command changes Version 5.4.9-2.1: command added to SBx908 GEN2

6

System Configuration and Monitoring Commands

- Contents**
- **Introduction** on page 185
 - **banner display external-manager** on page 186
 - **banner exec** on page 187
 - **banner external-manager** on page 189
 - **banner login (system)** on page 191
 - **banner motd** on page 192
 - **clock set** on page 194
 - **clock summer-time date** on page 195
 - **clock summer-time recurring** on page 197
 - **clock timezone** on page 200
 - **debug core-file** on page 201
 - **findme** on page 202
 - **hostname** on page 203
 - **low-memory restart** on page 205
 - **max-fib-routes** on page 206
 - **max-static-routes** on page 208
 - **no debug all** on page 209
 - **reboot** on page 211
 - **receive-packet-scheduler** on page 212
 - **reload** on page 214
 - **show banner external-manager** on page 215
 - **show clock** on page 216
 - **show cpu** on page 218
 - **show cpu history** on page 221
 - **show debugging** on page 223
 - **show interface memory** on page 224
 - **show memory** on page 226
 - **show memory allocations** on page 229
 - **show memory history** on page 231
 - **show memory pools** on page 232
 - **show memory shared** on page 233
 - **show process** on page 234
 - **show reboot history** on page 237
 - **show router-id** on page 238
 - **show system** on page 239
 - **show system environment** on page 240
 - **show system environment counters** on page 241

- **show system interrupts** on page 243
- **show system mac** on page 244
- **show system pci device** on page 245
- **show system pci tree** on page 246
- **show system serialnumber** on page 247
- **show tech-support** on page 248
- **speed (asyn)** on page 251
- **terminal monitor** on page 253
- **undebug all** on page 254

Introduction

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

banner display external-manager

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

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

Syntax banner display external-manager
no banner display external-manager

Default The external-manager banner is displayed by default.

Mode User Exec

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

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

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

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

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

Related commands [banner external-manager](#)
[show banner external-manager](#)

Command changes Version 5.5.1-1.1: command added

banner exec

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

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

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

AlliedWare Plus (TM) 5.5.5 04/05/26 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) 5.5.5 04/05/26 12:00:00

awplus>
```

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

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

awplus login: manager
Password:

awplus>
```

Related commands [banner login \(system\)](#)
[banner motd](#)

banner external-manager

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

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

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

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

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

Mode Global Configuration

Usage notes When you run this command:

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

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

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

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

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

```
awplus# configure terminal
```

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

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

```
awplus# configure terminal
```

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

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

```
awplus# configure terminal
```

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

Related commands **banner display external-manager**
show banner external-manager

Command changes Version 5.5.1-1.1: command added

banner login (system)

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

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

Syntax banner login
no banner login

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

Mode Global Configuration

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

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

Authorised users only

awplus(config)#exit
awplus#exit

Authorised users only

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.5 04/05/26 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) 5.5.5 04/05/26 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) 5.5.5 04/05/26 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) 5.5.5 04/05/26 12:00:00

awplus>
```

Related **banner exec**
commands **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**).

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
<code><timezone-name></code>	A description of the summertime zone, up to 6 characters long.
<code>date</code>	Specifies that this is a date-based summertime setting for just the specified year.
<code><start-day></code>	Day that the summertime starts, from 1 to 31.
<code><start-month></code>	First three letters of the name of the month that the summertime starts.
<code><start-year></code>	Year that summertime starts, from 2000 to 2035.
<code><start-time></code>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<code><end-day></code>	Day that summertime ends, from 1 to 31.
<code><end-month></code>	First three letters of the name of the month that the summertime ends.
<code><end-year></code>	Year that summertime ends, from 2000 to 2035.
<code><end-time></code>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<code><1-180></code>	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**) and recurring dates.

By default, the device has no summertime definitions set.

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

no clock summer-time

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

Mode Global Configuration

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

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

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

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

Related commands [clock summer-time date](#)
[clock timezone](#)

clock timezone

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

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

By default, the system time is set to UTC.

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related commands [clock set](#)
[clock summer-time date](#)
[clock summer-time recurring](#)

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

findme

Overview Use this command to physically locate a specific device from a group of similar devices. Activating the command causes the wireless LEDs to flash. Use the **no** variant of this command to deactivate the Find Me feature prior to the timeout expiring.

Syntax findme [timeout <duration>]
no findme

Parameter	Description
timeout <duration>	How long the LEDs flash, in seconds, in the range 5 to 3600 seconds. If you specify this, normal LED behavior is restored automatically after the specified time has elapsed, or a no findme command is used.

Default By default the wireless LEDs flash for 60 seconds.

Mode Privileged Exec

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

```
awplus# findme
```

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

```
awplus# findme timeout 120
```

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

```
awplus# no findme
```

hostname

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

- displayed in the output of the **show system** command
- displayed in the CLI prompt so you know which device you are configuring

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><hostname></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.

This command does not set the sysName MIB value. The hostname and the sysName MIB value are independent of each other. Use the **snmp-server system-name** command to set the MIB value.

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

```
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](#)
[snmp-server system-name](#)

Command changes Version 5.5.5-2.1: command no longer sets the sysName MIB value.

low-memory restart

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

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

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

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

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

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

Mode Global Configuration

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

Example To specify RIP as the process to terminate if memory gets too low, use the commands:

```
awplus# configure terminal
awplus(config)# low-memory restart ripd
```

Related commands [show memory](#)
[snmp-server enable trap](#)

Command changes Version 5.5.4-2.3: command added

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:

*When using VRF-lite, this command applies to the Global VRF instance; to set the max-fib-routes for a user-defined VRF instance use the **max-fib-routes (VRF)** command. For static routes use the **max-static-routes** command for the Global VRF instance and the **max-static-routes (VRF)** command for a user-defined VRF instance.*

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

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

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

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

Mode Global Configuration

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

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

Related commands [max-fib-routes \(VRF\)](#)

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 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 ospf|ipv6 rip|dot1x|nsm|ospf|pim dense-mode|pim sparse-mode|rip|vrrp]`

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

Default Disabled

Mode Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

To disable all NSM debugging, use the command:

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

Related commands **undebug all**

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

reboot

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

Syntax reboot
reload

Mode Privileged Exec

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

Examples To restart the device, use the command:

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

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 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
Command
changes**

show running-config

Version 5.4.8-2.1: command added

reload

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

show banner external-manager

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

Syntax show banner external-manager

Mode User Exec

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

```
awplus# show banner external-manager
```

Output The following shows typical output.

Example output from show banner external-manager

```
awplus#show banner external-manager
The following features are being managed by external systems.
Configuring these features may have unintended consequences.
Manager: Network Manager
  Feature: ACLs
  Filters

Manager: Vista Manager
  Feature: Traffic control
  Application Priority
  Dynamic Traffic Management
  Feature: Web control
  all features
```

Related commands [banner display external-manager](#)
[banner external-manager](#)

Command changes Version 5.5.1-1.1: command added

show clock

Overview This command displays the system's current configured local time and date. It also displays other clock related information such as timezone and summertime configuration.

Syntax show clock

Mode User Exec and Privileged Exec

Example To display the system's current local time, use the command:

```
awplus# show clock
```

Output The following shows typical output.

Example output from the show c lock 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
```

Parameters in the output of the show c lock 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 Test paragraph

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 The following shows typical output.

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 mtddbldk0       0.0    20  sleep    0        5
 93 sync_supers     0.0    20  sleep    0        1
```

Parameters in the output of the show cpu command

Parameter	Description
CPU averages	Average CPU utilization for the periods stated.

Parameter	Description
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:

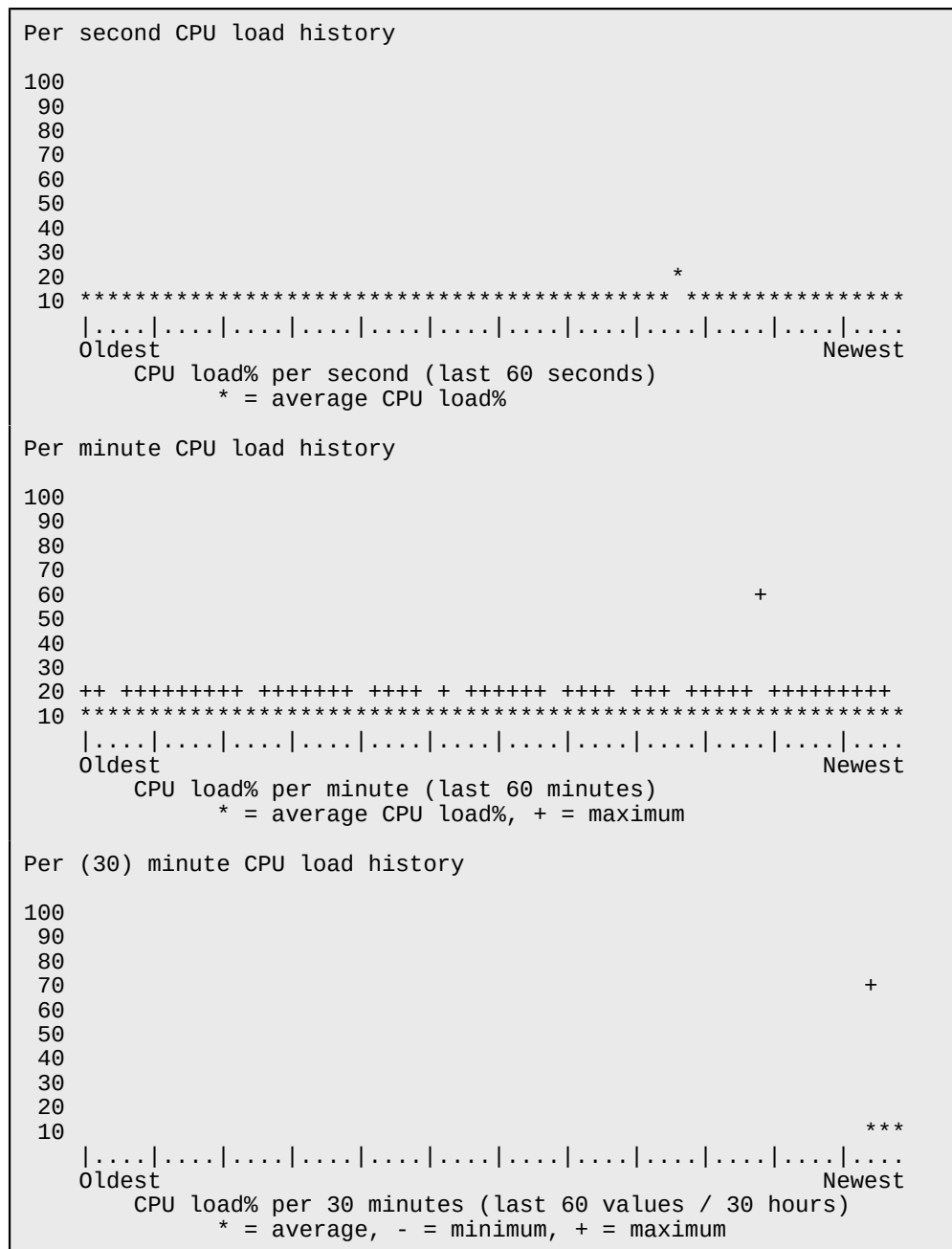
- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

Examples To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

Output The following shows typical output.

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 The following shows typical output.

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
<i><port-list></i>	Display information about only the specified port or ports. The port list can be: • an Eth port (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where ‘10’ is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth1-eth2) • a comma-separated list (e.g. eth1,eth2). Do not mix interface types in a list.

Mode User Exec and Privileged Exec

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

```
awplus# show interface memory
```

To display the shared memory used by eth0, use the command:

```
awplus# show interface eth0 memory
```

Output The following shows typical output.

Example output from the show interface memory command

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

Interface	shmid	Bytes Used	nattch	Status
eth1	393228	512	1	
eth2	458766	512	1	
lo	425997	512	1	
br1	557073	512	1	
ppp0	589842	512	1	

Example output from show interface <port-list> memory for a list of interfaces

```
awplus#show interface eth1-2 memory
Vlan blocking state shared memory usage
-----
```

Interface	shmid	Bytes Used	nattch	Status
eth1	393228	512	1	
eth2	458766	512	1	

Related commands [show interface brief](#)
[show interface status](#)

show memory

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

For information on filtering and saving command output, see the [Getting Started with the AlliedWare Plus Command Line Interface](#).

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

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

Mode User Exec and Privileged Exec

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

```
awplus# show memory
```

Output The following shows typical output.

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
...
```

Parameters in the output of the show memory command

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

Related commands

- low-memory restart**
- show memory allocations**
- show memory history**
- show memory pools**
- show memory shared**
- snmp-server enable trap low-memory**

show memory allocations

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

Syntax show memory allocations [<process>]

Parameter	Description
<process>	Displays the memory allocation used by the specified process.

Mode User Exec and Privileged Exec

Example To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

Output The following shows typical output.

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 The following shows typical output.

Example output from the show memory history command

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

Related commands

- [show memory allocations](#)
- [show memory pools](#)
- [show memory shared](#)
- [show tech-support](#)

show memory pools

Overview This command shows the memory pools used by processes.

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

Syntax show memory pools [*<process>*]

Parameter	Description
<i><process></i>	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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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
...
```

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.

Parameter	Description
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 The following shows typical output.

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
```

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 The following shows typical output.

Example output from the show router-id command

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

show system

Overview Use this command to display general system information about the device, including the hardware, memory usage, and software version. It also displays location and contact details when these have been set.

For information on filtering and saving command output, see the [Getting Started with the AlliedWare Plus Command Line Interface](#).

Syntax show system

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Output The following shows typical output.

Example output from show system

```
awplus#show system
System Status                                     Tue May 06 02:31:43 2025

Board      ID   Bay      Board Name                      Rev   Serial number
-----
Base       657  Base     AT-TQ7403-R                    A-0   A10581R232800069
-----
RAM: Total: 1854040 kB Free: 1259308 kB
Flash: 393.7MB Used: 312.7MB Available: 81.0MB
-----
Environment Status : Normal
Uptime             : 7 days 05:47:45
Bootloader version : Unknown

Current software   : TQ7403R-5.5.4-2.3.rel
Software version   : 5.5.4-2.3
Build date         : Mon Apr 28 09:06:53 UTC 2025

Current boot config: flash:/default.cfg (file exists)
System Name
awplus
System Contact
System Location
```

show system environment

Overview Use this command to display the current environmental status of your device and its power supplies and any other expansion options. The environmental status covers information about temperatures, fans, and voltage.

For information on filtering and saving command output, see the [Getting Started with the AlliedWare Plus Command Line Interface](#).

Syntax show system environment

Mode User Exec and Privileged Exec

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

```
awplus# show system environment
```

Output The following shows typical output.

Example output from show system environment

```
awplus#show system environment
Environment Monitoring Status

Overall Status: Normal

Resource ID: 1  Name: AT-TQ7403-R
ID  Sensor (Units)          Reading  Low Limit  High Limit  Status
1   AC: On                  Yes      -          -           Ok
2   POE-ETH1: On            No       -          -           Ok
3   POE-ETH2: On            No       -          -           Ok
4   Temp: NSS top (Degrees C)  43      -          -           Ok
5   Temp: NSS UBI32_0 (Degrees C)  43      -          -           Ok
6   Temp: WCSS PHYA_0 (Degrees C)  43      -          -           Ok
7   Temp: WCSS PHYA_1 (Degrees C)  43      -          -           Ok
8   Temp: A53 MHM (Degrees C)    44      -          -           Ok
9   Temp: LPASS QDSP6 (Degrees C)  43      -          -           Ok
10  Temp: top (Degrees C)       44      -          -           Ok
```

Related commands [show system](#)
[show system environment counters](#)
[trigger](#)
[type env-sensor](#)

show system environment counters

Overview Use this command to see the environmental sensor counters.

Syntax show system environment counters

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

Example output from show system environment counters

```
awplus#show system environment counters

Resource ID: 1  Name: AT-TQ7403-R
ID Sensor      Value      Threshold  Checked  Read   Alarm   Alarm
               readings readings readings errors asserted cleared
1  AC: On      6          0          0        1      0        0
2  POE-ETH1: On 0          0          0        6      0        0
3  POE-ETH2: On 0          0          0        6      0        0
4  Temp: NSS top 6          0          0        0      0        0
5  Temp: NSS UBI32_0 6          0          0        0      0        0
6  Temp: WCSS PHYA_0 6          0          0        0      0        0
7  Temp: WCSS PHYA_1 6          0          0        0      0        0
8  Temp: A53 MHM 6          0          0        0      0        0
9  Temp: LPASS QDSP6 6          0          0        0      0        0
10 Temp: top    6          0          0        0      0        0
```

Parameters in the output from show system environment counters

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

Related commands [show system](#)
[show system environment](#)

Command changes Version 5.5.0-0.1: command added

show system interrupts

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

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

Syntax show system interrupts

Mode User Exec and Privileged Exec

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

```
awplus# show system interrupts
```

Output The following shows typical output.

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 The following shows typical output.

Example output from the show system mac command

```
awplus#show system mac
0200.0034.5682 (eth1)
0200.0034.5683 (eth2)
0200.0034.5684 (system)
```


show system pci device

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

Syntax show system pci device

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

Example output from the show system pci device command

```
awplus#show system pci device
00:0c.0 Class 0200: 11ab:00d1 (rev 01)
      Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 113
      Memory at 5ffff000 (32-bit, non-prefetchable) [size=4K]
      Memory at 58000000 (32-bit, non-prefetchable) [size=64M]

00:0d.0 Class 0200: 11ab:00d1 (rev 01)
      Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 116
      Memory at 57fff000 (32-bit, non-prefetchable) [size=4K]
      Memory at 50000000 (32-bit, non-prefetchable) [size=64M]
```

Related commands [show system pci tree](#)

show system pci tree

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

Syntax show system pci tree

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

Example output from the show system pci tree command

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

Related commands [show system 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 The following shows typical output.

Example output from the show system serialnumber command

```
awplus#show system serialnumber
45AX5300X
```

show tech-support

Overview This command generates system and debugging information for the device and saves it to a file.

This command is useful for collecting a large amount of information so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

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

Syntax show tech-support {[all|atmf|auth|bgp|card|dhcpsn|epsr|firewall|igmp|ip|ipv6|mld|openflow|ospf|ospf6|pim|rip|ripng|stack|stp|system|tacacs+|update]} [outfile <filename>]

Parameter	Description
all	Display full information
atmf	Display ATMF-specific information
auth	Display authentication-related information
bgp	Display BGP-related information
card	Display Chassis Card specific information
dhcpsn	Display DHCP Snooping specific information
epsr	Display EPSR specific information
firewall	Display firewall specific information
igmp	Display IGMP specific information
ip	Display IP specific information
ipv6	Display IPv6 specific information
mld	Display MLD specific information
openflow	Display information related to OpenFlow
ospf	Display OSPF related information
ospf6	Display OSPF6 specific information
pim	Display PIM related information
rip	RIP related information
ripng	Display RIPNG specific information
stack	Display stacking device information
stp	Display STP specific information
system	Display general system information
tacacs+	Display TACACS+ information
update	Display resource update specific information
	Output modifier

Parameter	Description
>	Output redirection
>>	Output redirection (append)
outfile	Output file name
<filename>	Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.

Default Captures **all** information for the device.

By default the output is saved to the file 'tech-support.txt.gz' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example 'tech-support20161009.txt.gz', so the previous file is retained.

Usage notes The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

Mode Privileged Exec

Examples To produce the output needed by technical support staff, use the command:

```
awplus# show tech-support
```

speed (asyn)

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

Syntax speed <console-speed-in-bps>

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

Default The default console speed baud rate is 9600 bps.

Mode Line Configuration

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

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

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

Then log in again to enable the change:

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

Related commands

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

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

- Contents**
- **Introduction** on page 257
 - **clear exception log** on page 258
 - **clear log** on page 259
 - **clear log buffered** on page 260
 - **clear log permanent** on page 261
 - **connection-log events** on page 262
 - **copy buffered-log** on page 263
 - **copy permanent-log** on page 264
 - **default log buffered** on page 265
 - **default log console** on page 266
 - **default log email** on page 267
 - **default log host** on page 268
 - **default log monitor** on page 269
 - **default log permanent** on page 270
 - **log buffered** on page 271
 - **log buffered (filter)** on page 272
 - **log buffered exclude** on page 277
 - **log buffered size** on page 281
 - **log console** on page 282
 - **log console (filter)** on page 283
 - **log console exclude** on page 288
 - **log date-format** on page 292
 - **log email** on page 294
 - **log email (filter)** on page 295
 - **log email exclude** on page 300
 - **log email time** on page 304
 - **log facility** on page 306
 - **log host** on page 308
 - **log host (filter)** on page 310
 - **log host exclude** on page 315
 - **log host source** on page 320
 - **log host startup-delay** on page 321
 - **log host time** on page 323
 - **log monitor (filter)** on page 326
 - **log monitor exclude** on page 331
 - **log permanent** on page 335
 - **log permanent (filter)** on page 336

- **log permanent exclude** on page 341
- **log permanent size** on page 345
- **log-rate-limit nsm** on page 346
- **log trustpoint** on page 348
- **log url-requests** on page 350
- **show connection-log events** on page 351
- **show counter log** on page 352
- **show exception log** on page 354
- **show log** on page 355
- **show log config** on page 357
- **show log permanent** on page 360
- **show running-config log** on page 362

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.

clear exception log

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

Syntax clear exception log

Mode Privileged Exec

Example awplus# clear exception log

clear log

Overview This command removes the contents of the buffered and permanent logs.

Syntax clear log

Mode Privileged Exec

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

```
awplus# clear log
```

Related commands

- [clear log buffered](#)
- [clear log permanent](#)
- [show log](#)

clear log buffered

Overview This command removes the contents of the buffered log.

Syntax clear log buffered

Mode Privileged Exec

Example To delete the contents of the buffered log use the following commands:

```
awplus# clear log buffered
```

Related commands

- [default log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

clear log permanent

Overview This command removes the contents of the permanent log.

Syntax clear log permanent

Mode Privileged Exec

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

```
awplus# clear log permanent
```

Related commands

- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent exclude](#)
- [log permanent size](#)
- [show log config](#)
- [show log permanent](#)

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><destination-name></code>	The filename and path for the destination file. See Introduction for valid syntax.

Mode Privileged Exec

Example To copy the buffered log file into a folder in Flash named “buffered-log” and name the file “buffered-log.log”, use the command:

```
awplus# copy buffered-log flash:/buffered-log/buffered-log.log
```

Related commands

- [log buffered](#)
- [show file systems](#)
- [show log](#)

Command changes Version 5.4.7-1.1: command added

copy permanent-log

Overview Use this command to copy the permanent log to an internal or external destination.

Syntax copy permanent-log <destination-name>

Parameter	Description
<destination-name>	The filename and path for the destination file. See Introduction for valid syntax.

Mode Privileged Exec

Example To copy the permanent log file into a folder in Flash named “perm-log” and name the file “permanent-log.log”, use the command:

```
awplus# copy permanent-log flash:/perm-log/permanent-log.log
```

Related commands

- [log permanent](#)
- [show file systems](#)
- [show log permanent](#)

Command changes Version 5.4.7-1.1: command added

default log buffered

Overview This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

Syntax default log buffered

Default The buffered log is enabled by default.

Mode Global Configuration

Example To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

Related commands

- clear log buffered**
- log buffered**
- log buffered (filter)**
- log buffered size**
- log buffered exclude**
- show log**
- show log config**

default log console

Overview This command restores the default settings for log messages sent to the terminal when a **log console** command is issued. By default all messages are sent to the console when a **log console** command is issued.

Syntax default log console

Mode Global Configuration

Example To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

Related commands

- log console**
- log console (filter)**
- log console exclude**
- show log config**

default log email

Overview This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax default log email *<email-address>*

Parameter	Description
<i><email-address></i>	The email address to send log messages to

Mode Global Configuration

Example To restore the default settings for log messages sent to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related commands

- [log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)

default log host

Overview This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax default log host *<ip-addr>*

Parameter	Description
<i><ip-addr></i>	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)

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	Filter messages to the buffered log by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from in the buffered log:
kern	Kernel messages

Parameter	Description
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text- string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the buffered log has a filter to select messages whose severity level is “notices (5)” or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

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

To remove a filter that sends all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

Related commands

- clear log buffered**
- default log buffered**
- log buffered**
- log buffered size**
- log buffered exclude**
- show log**
- show log config**

log buffered exclude

Overview Use this command to exclude specified log messages from the buffered log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax log buffered exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log buffered exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]

Parameter	Description																
level	Exclude messages of the specified severity level.																
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (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

Parameter	Description
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>

Parameter	Description
<50-250>	Size of the permanent 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**

Command changes Version 5.5.3-2.1: Maximum and default size increased on AMFCloud and AR4000S-Cloud

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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
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

Parameter	Description
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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (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

Parameter	Description
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 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><email-address></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 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 specified email address. All configuration relating to this log target will be removed.

Syntax log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
no log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]

Parameter	Description																
<email- address>	The email address to send logging messages to																
level	Filter messages by severity level.																
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)						
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	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages

Parameter	Description
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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (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

Parameter	Description
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 email exclude msgtext example of irrelevant message
```

Related commands

- [default log email](#)
- [log email](#)
- [log email \(filter\)](#)
- [log email time](#)
- [show log config](#)

log email time

Overview This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

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

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

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

Examples To send messages to the email address `test@home.com` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus
3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus
3
```

Related commands

- default log email**
- log email**
- log email (filter)**
- log email exclude**
- show log config**

log facility

Overview Use this command to assign a facility to all log messages generated on this device. This facility overrides any facility that is automatically generated as part of the log message.

Use the **no** variant of this command to remove the configured facility.

Syntax `log facility {kern|user|mail|daemon|auth|syslog|lpr|news|uucp|cron|authpriv|ftp|local0|local1|local2|local3|local4|local5|local6|local7}`
`no log facility`

Default None. The outgoing syslog facility depends on the log message.

Mode Global Configuration

Usage notes Specifying different facilities for log messages generated on different devices can allow messages from multiple devices sent to a common server to be distinguished from each other.

Ordinarily, the facility values generated in log messages have meanings as shown in the following table. Using this command will override these meanings, and the new meanings will depend on the use you put them to.

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
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>`

Syntax (VRF-lite) `log host <ipv4-addr>|<ipv6-addr> [vrf <vrf-name>] [secure]`
`no log host <ipv4-addr>|<ipv6-addr> [vrf <vrf-name>]`

Parameter	Description
<code><ipv4-addr></code>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<code><ipv6-addr></code>	Specify the source IPv6 address, in X:X::X:X notation.
<code>vrf <vrf-name></code>	The name of a VRF instance. Use this to specify the VRF that the remote syslog server (host) is accessible by. Hosts are uniquely identified by their address and VRF, so multiple hosts can have the same address as long as the VRF is different. The default is the global VRF.
<code>secure</code>	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
```

Example (VRF-lite) To configure the device to send log messages to a remote syslog server that is accessible via VRF 'red', use the following commands:

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

Related commands

- default log host**
- log host (filter)**
- log host exclude**
- log host source**
- log host startup-delay**
- log host time**
- log trustpoint**
- show log config**

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host (filter)

Overview This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

Syntax `log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Syntax (VRF-lite) `log host <ip-addr> [vrf <vrf-name>] [level <level>]
[program <program-name>] [facility <facility>] [msgtext <text-string>]
no log host <ip-addr> [vrf <vrf-name>] [level <level>]
[program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<code><ip-addr></code>	The IP address of a remote syslog server.																
<code>vrf <vrf-name></code>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.																
<code>level</code>	Filter messages by severity level.																
<code><level></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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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><program- name></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. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
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

Parameter	Description
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:

```
awplusawplus# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Example (VRF-lite) 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, when that server is in VRF ‘red’, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 vrf red level informational
```

Related commands

- [default log host](#)
- [log host](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host exclude

Overview Use this command to prevent specified log messages from being sent to the remote syslog server, when **log host** is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude
[level <level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]
no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude
[level <level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]`

Syntax (VRF-lite) `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<hostname>	The host name of a remote syslog server.																
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.																
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.																
vrf <vrf-name>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.																
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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)						
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

Parameter	Description
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 exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 exclude msgtext example of
irrelevant message
```

Example (VRF-lite) To exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, within VRF 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 vrf red exclude msgtext
example of irrelevant message
```

Related commands

- default log host**
- log host**
- log host (filter)**
- log host source**
- log host time**
- show log config**

Command changes Version 5.2.2-1.1: **vrf** parameter added for products that support VRF

log host source

Overview Use this command to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

Note that AlliedWare Plus does not support source interface settings on secure log hosts (which are hosts configured using "log host <ip-address> secure").

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

Syntax log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}
no log host source

Parameter	Description
<interface-name>	Specify the source interface name. You can enter an Eth interface or loopback interface.
<ipv4-addr>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<ipv6-addr>	Specify the source IPv6 address, in X:X::X:X notation.

Default None (no source is configured)

Mode Global Configuration

Example To send syslog messages from 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host source 192.168.1.1
```

Related commands

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host time](#)
- [show log config](#)

log host startup-delay

Overview Use this command to set the delay between the device booting up and it attempting to connect to remote log hosts. This is to allow time for network connectivity to the remote host to be established. During this period, the device buffers log messages and sends them once it has connected to the remote host.

The startup delay begins when the message "syslog-ng starting up" appears in the log.

If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In these cases, you can use the command to increase the startup delay.

Use the **no** variant of this command to return to the default delay values.

Syntax log host startup-delay [delay <1-600>] [messages <1-5000>]
no log host startup-delay

Parameter	Description
delay <1-600>	The time, in seconds, from when syslog starts before the device attempts to filter and transmit the buffered messages to remote hosts.
messages <1-5000>	The maximum number of messages that the device will buffer during the delay period.

Default By default the system will buffer up to 2000 messages and wait 120 seconds from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts.

Mode Global Configuration

Example To increase the delay to 180 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# log host startup-delay delay 180
```

Related commands

- default log host**
- log host (filter)**
- log host exclude**
- log host source**
- log host time**
- log trustpoint**
- show log config**

Command changes Version 5.4.8-0.2: defaults changed

log host time

Overview This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} time {local|local-offset|utc-offset {plus|minus} <0-24>}`

Syntax (VRF-lite) `log host {<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] time {local|local-offset|utc-offset {plus|minus} <0-24>}`

Parameter	Description
<code><hostname></code>	The host name of a remote syslog server.
<code><ipv4-addr></code>	The IPv4 address of a remote syslog server, in A.B.C.D format.
<code><ipv6-addr></code>	The IPv6 address of a remote syslog server, in X:X::X:X format.
<code><email-address></code>	The email address to send log messages to
<code>vrf <vrf-name></code>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.
<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 plus or minus 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 plus or minus keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
<code>plus</code>	Negative offset (difference) from the device to the syslog server.
<code>minus</code>	Positive offset (difference) from the device to the syslog server.
<code><0-24></code>	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
```

Example (VRF-lite) To send messages to the remote syslog server with the IP address 10.32.16.02 within the VRF 'red', in the same time zone as the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 vrf red time utc-offset
minus 3
```

Related commands

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [show log config](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log monitor (filter)

Overview This command creates a filter to select messages to be sent to the terminal when the **terminal monitor** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax log monitor [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log monitor [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]

Parameter	Description																
level	Filter messages by severity level.																
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
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

Parameter	Description
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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (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

Parameter	Description
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 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)

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
poel	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
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

Parameter	Description
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text- string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the buffered log has a filter to select messages whose severity level is notices (5) or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To create a filter to send all messages containing the text "Bridging initialization", to the permanent log use the following commands:

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

Related commands

- clear log permanent**
- default log permanent**
- log permanent**
- log permanent exclude**
- log permanent size**
- show log config**
- show log permanent**

log permanent exclude

Overview Use this command to prevent specified log messages from being sent to the permanent log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log permanent exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log permanent exclude [level <level>] [program <program-
name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																
level	Exclude messages of the specified severity level.																
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (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

Parameter	Description
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Exclude messages containing a certain text string.
<text- string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent exclude msgtext example of
irrelevant message
```

Related commands

- [clear log permanent](#)
- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent size](#)
- [show log config](#)
- [show log permanent](#)

log permanent size

Overview This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled, old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

Syntax log permanent size <50-250>

no log permanent size

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

Default 50 kilobytes

Mode Global Configuration

Example To allow the permanent log to use up to 100 kilobytes of NVS, use the commands:

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

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log permanent size
```

Related commands

- [clear log permanent](#)
- [copy permanent-log](#)
- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent exclude](#)
- [show log config](#)
- [show log permanent](#)

Command changes Version 5.5.3-2.1: Maximum and default size increased on AMFCloud and AR4000S-Cloud

log-rate-limit nsm

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

Use the **no** variant of this command to revert to the default number of log messages, which is up to 200 log messages per second.

Syntax `log-rate-limit nsm messages <message-limit> interval <time-interval>`
`no log-rate-limit nsm`

Parameter	Description
<code><message-limit></code>	<code><1-65535></code> The number of log messages generated by the device.
<code><time-interval></code>	<code><0-65535></code> The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied.

Default By default, the device will allow 200 log messages to be generated per second.

Mode Global Configuration

Usage notes This command limits the rate that log messages are generated. Limiting log messages protects the device from running out of memory in extreme conditions, such as during a broadcast storm.

Once the specified number of log messages per interval is exceeded, any excess log messages are dropped. When this occurs a summary log message is generated at the end of the interval. This summary message includes the number of log messages dropped.

If you expect a lot of dropped log messages, we recommend setting the time interval to no less than 100. This limits the number of summary messages to one per second, which prevents the log from filling up with these summary messages.

Examples To allow the device to generate a maximum of 300 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# log-rate-limit nsm messages 300 interval 100
```

To return the device to the default setting, use the following commands:

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

log trustpoint

Overview This command adds one or more trustpoints to be used with the syslog application. Multiple trustpoints may be specified, or the command may be executed multiple times, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax log trustpoint [*<trustpoint-list>*]
no log trustpoint [*<trustpoint-list>*]

Parameter	Description
<i><trustpoint-list></i>	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 **log host**
commands **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 The following shows typical output.

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 The following shows typical output.

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

Parameters in output of the show counter log command

Parameter	Description
Total Received	Total number of messages received by the log
Total Received P0	Total number of Priority 0 (Emergency) messages received
Total Received P1	Total number of Priority 1 (Alert) messages received
Total Received P2	Total number of Priority 2 (Critical) messages received
Total Received P3	Total number of Priority 3 (Error) messages received
Total Received P4	Total number of Priority 4 (Warning) messages received
Total Received P5	Total number of Priority 5 (Notice) messages received
Total Received P6	Total number of Priority 6 (Info) messages received
Total Received P7	Total number of Priority 7 (Debug) messages received

Related commands [show log config](#)

show exception log

Overview This command displays the contents of the exception log. If the device has unexpectedly restarted and has produced a core dump file, the output of this command shows the name and location of the file.

Syntax show exception log

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output The following shows typical output.

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 The following shows typical output.

Example output from show log

```
awplus#show log
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2025 Apr 28 20:44:57 kern.notice awplus kernel: [ 0.000000] Linux version 5.4.164
(maker@maker34-build) (gcc version 13.2.0 (crosstool-NG 1.26.0_dirty)) #1 SMP
PREEMPT Wed Apr 16 07:19:59 UTC 2025
2025 Apr 28 20:44:57 syslog.notice awplus syslog-ng[493]: syslog-ng starting up;
version='3.21.1'
2025 Apr 28 20:44:57 kern.warning awplus kernel: [ 0.000000]
ARM_SMCCC_ARCH_WORKAROUND_1 missing from firmware
2025 Apr 28 20:44:57 kern.notice awplus kernel: [ 0.000000] Kernel command
line: console=ttyMSM0,115200n8 cnss2.bdf_pci0=0xa7 loglevel=1 root=/dev/ram0
mtdoops.mtddev=errlog swiotlb=1 softdog.soft_panic=1...
```

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 The following shows typical output.

Example output from show log config

```
Facility: default
PKI trustpoints: example_trustpoint

Buffered log:
Status ..... enabled
Maximum size ... 100kb
Filters:
*1 Level ..... notices
  Program ..... any
  Facility ..... any
  Message text . any
  2 Level ..... informational
    Program ..... auth
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2016 Oct 11
10:36:16)

Permanent log:
Status ..... enabled
Maximum size ... 60kb
Filters:
1 Level ..... error
  Program ..... any
  Facility ..... any
  Message text . any
*2 Level ..... warnings
  Program ..... dhcp
  Facility ..... any
  Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2016 Oct 11
10:36:16)

Host 10.32.16.21:
Time offset .... +2:00
Offset type .... UTC
Source ..... -
Secured ..... enabled
Filters:
1 Level ..... critical
  Program ..... any
  Facility ..... any
  Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2016 Oct 11
10:36:16)

Email admin@alliedtelesis.com:
Time offset .... +0:00
Offset type .... Local
Filters:
1 Level ..... emergencies
  Program ..... any
  Facility ..... any
  Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2016 Oct 11
10:36:16)
...
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with '*'.

NOTE: *Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.*

Related commands

- show counter log**
- show log**
- show log permanent**

show log permanent

Overview This command displays the contents of the permanent log.

Syntax show log permanent [tail [<10-250>]]

Parameter	Description
tail	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the **tail** parameter to change how many of the latest messages should be displayed.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the permanent log, use the command:

```
awplus# show log permanent
```

Output The following shows typical output.

Example output from show log permanent

```
awplus#show log permanent
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2025 Mar 24 19:07:57 kern.warning awplus kernel: [2318892.661458] IPv4: martian
source 10.37.179.6 from 10.37.179.14, on dev eth1.179
2025 Mar 24 19:07:57 kern.warning awplus kernel: [2318892.661461] ll header:
00000000: ff ff ff ff ff ff 88 9d 98 53 ad e0 08 06 00 01
2025 Mar 24 19:07:57 kern.warning awplus kernel: [2318892.661464] ll header:
00000010: 08 00
2025 Mar 24 19:07:57 kern.warning awplus kernel: [2318892.661528] IPv4: martian
source 10.37.179.6 from 10.37.179.14, on dev eth1.179
```

Related commands

- clear log permanent**
- copy permanent-log**
- default log permanent**
- log permanent**
- log permanent (filter)**
- log permanent exclude**
- log permanent size**
- show log config**

show running-config log

Overview This command displays the current running configuration of the Log utility.

Syntax show running-config log

Mode Privileged Exec and Global Configuration

Example To display the current configuration of the log utility, use the command:

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

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

8

Scripting Commands

- Contents**
- **Introduction** on page 364
 - **activate** on page 365
 - **echo** on page 367
 - **wait** on page 368

Introduction

Overview This chapter provides commands used for command scripts.

Command List

activate

Overview This command activates a script file.

Syntax activate [background] <script>

Parameter	Description
background	Activate a script to run in the background. A process that is running in the background will operate as a separate task, and will not interrupt foreground processing. Generally, we recommend running short, interactive scripts in the foreground and longer scripts in the background. The default is to run the script in the foreground.
<script>	The file name of the script to activate. The script is a command script consisting of commands documented in this software reference. Note that you must use either a .scp or a .sh filename extension for a valid script text file, as described below in the usage section for this command.

Mode Privileged Exec

Usage notes When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an **enable (Privileged Exec mode)** command to the start of your script. If you need to run Global Configuration commands in your script you need to add a **configure terminal** command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A **terminal length** shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **.sh** or **.scp** only for the AlliedWare Plus CLI to activate the script file. The **.sh** filename extension indicates the file is an ASH script, and the **.scp** filename extension indicates the file is an AlliedWare Plus script.

Examples To activate a command script to run as a background process, use the command:

```
awplus#activate background test.scp
```

Related commands

- configure terminal**
- echo**
- enable (Privileged Exec mode)**
- wait**

echo

Overview This command echoes a string to the terminal, followed by a blank line.

Syntax `echo <line>`

Parameter	Description
<line>	The string to echo

Mode User Exec and Privileged Exec

Usage This command may be useful in CLI scripts, to make the script print user-visible comments.

Example To echo the string Hello World to the console, use the command:

```
awplus# echo Hello World
```

Output

```
Hello World
```

Related commands [activate](#)
[wait](#)

wait

Overview This command pauses execution of the active script for the specified period of time.

Syntax wait <delay>

Parameter	Description
<delay>	<1 - 65535> Specify the time delay in seconds

Default No wait delay is specified by default.

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

Usage notes Use this command to pause script execution in an **.scp** (AlliedWare Plus™ script) or an **.sh** (ASH script) file executed by the **activate** command. The script must contain an **enable** command, because the **wait** command is only executed in the Privileged Exec mode.

Example See an **.scp** script file extract below that will show port counters for interface eth1 over a 10 second interval:

```
enable
show interface eth1
wait 10
show interface eth1
```

Related commands **activate**
echo
enable (Privileged Exec mode)

9

Interface Commands

- Contents**
- **Introduction** on page 370
 - **description (interface)** on page 371
 - **interface (to configure)** on page 372
 - **ip tcp adjust-mss** on page 374
 - **ipv6 tcp adjust-mss** on page 376
 - **mtu** on page 378
 - **service statistics interfaces counter** on page 380
 - **show interface** on page 381
 - **show interface brief** on page 384
 - **show interface memory** on page 386
 - **show interface status** on page 388
 - **shutdown** on page 390

Introduction

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

description (interface)

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

Syntax `description <description>`

Parameter	Description
<code><description></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 an interface is connected to.

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# description Master Link
```

Command changes Version 5.4.7-1.1: valid character set changed to printable ASCII characters

interface (to configure)

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

Syntax `interface <interface-list>`

Parameter	Description
<code><interface-list></code>	The interfaces to configure. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. The specified interfaces must exist.

Usage notes A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

Mode Global Configuration

Examples The following example shows how to enter Interface mode to configure the Ethernet interface eth0.2. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface eth0.2
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the 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
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	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

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
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	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.

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 eth interface default is 1500 bytes.

Syntax mtu <68-1582>
no mtu

Parameter	Description
<68-1582>	The Maximum Transmission size in bytes.

Default The default MTU size, for example 1500 bytes for eth 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

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth0 with MTU 1200 and tunnel1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Examples To configure an MTU size of 1555 bytes for tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1555
```

To restore the MTU size to the default MTU size of 1500 bytes on tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no mtu
```

Related commands [show interface](#)

Command changes Version 5.4.7-1.1: Behavior change when MTU set to less than 1500 on FS980M and GS980M.

Version 5.5.1-0.1: Layer 3 jumbo frames supported on SBx908 GEN2 and x950.

Version 5.5.1-1.2: Layer 3 jumbo frames supported on x530 and GS980MX.

Version 5.5.3-1.x Layer 3 jumbo frames supported on x240, SE240, x250, SE250, x540L, SE540L.

Version 5.5.5-0.1 Layer 3 jumbo frames supported on XS900MX, x550, x930, SBx81CFC960.

service statistics interfaces counter

Overview Use this command to enable the interface statistics counter.
Use the **no** variant of this command to disable the interface statistics counter.

Syntax service statistics interfaces counter
no service statistics interfaces counter

Default The interface statistics counter is enabled by default.

Mode Global Configuration

Example To enable the interface statistics counter, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# service statistics interfaces counter
```

To disable the interface statistics counter, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no service statistics interfaces counter
```

Command changes Version 5.4.7-2.1: command added

show interface

Overview Use this command to display interface configuration and status.

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

Syntax show interface [<interface-list>]

Parameter	Description
<interface-list>	The interfaces or ports to display. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

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

```
awplus# show interface
```

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

```
awplus# show interface lo
```

To display configuration and status information for br1, use the command:

```
awplus# show interface br1
```

To display configuration and status information for eth1, use the command:

```
awplus# show interface eth1
```

Output The following shows typical output.

Example output from the show interface command:

```
awplus#show interface
Interface eth1
  Link is UP, administrative state is UP
  Hardware is Ethernet, address is 889d.9853.ade0
  index 8 metric 1 mtu 1500
  current duplex full, current speed 1000, current polarity auto
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,RUNNING,ALLMULTI,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 567326928, bytes 58165706877, dropped 0, multicast packets 1977063
    output packets 5681528, bytes 2962262952
    input average rate : 30 seconds 5.53 Kbps, 5 minutes 5.42 Kbps
    output average rate: 30 seconds 2.23 Kbps, 5 minutes 2.60 Kbps
    input peak rate 109.54 Gbps at 2025/03/25 13:12:22
    output peak rate 145.62 Mbps at 2025/03/25 13:12:22
  Time since last state change: 45 days 02:12:51
  ...
```

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
```

Example output from the show interface br command:

```
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
```

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 [mtu](#)
[show interface brief](#)
[show interface status](#)

Command changes Version 5.4.7-2.1: average rate and peak rate added to output

show interface brief

Overview Use this command to display brief interface, configuration, and status information, including provisioning information.

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

Syntax show interface brief

Mode User Exec and Privileged Exec

Example To display summarized information about all interfaces on the device, use the command:

```
awplus# show interface brief
```

Output The following shows typical output.

Example output from show interface brief

awplus#show interface brief		
Interface	Status	Protocol
eth1	admin up	running
eth1.179	admin up	running
eth2	admin up	down
lo	admin up	running
br0	admin up	running
vap1.0	admin up	running
vap1.1	admin up	running
vap1.2	admin up	running
vap1.3	admin up	running
vap1.4	admin up	running
vap1.5	admin up	running

Parameters in the output of show interface brief

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

Related **show interface**
commands **show interface status**
show interface memory

show interface memory

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

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

Syntax show interface memory
show interface *<port-list>* memory

Parameter	Description
<i><port-list></i>	Display information about only the specified port or ports. The port list can be: • an Eth port (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where ‘10’ is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth1-eth2) • a comma-separated list (e.g. eth1,eth2). Do not mix interface types in a list.

Mode User Exec and Privileged Exec

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

```
awplus# show interface memory
```

To display the shared memory used by eth0, use the command:

```
awplus# show interface eth0 memory
```

Output The following shows typical output.

Example output from the show interface memory command

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

Interface	shmid	Bytes Used	nattch	Status
eth1	393228	512	1	
eth2	458766	512	1	
lo	425997	512	1	
br1	557073	512	1	
ppp0	589842	512	1	

Example output from show interface <port-list> memory for a list of interfaces

```
awplus#show interface eth1-2 memory
Vlan blocking state shared memory usage
-----
```

Interface	shmid	Bytes Used	nattch	Status
eth1	393228	512	1	
eth2	458766	512	1	

Related commands [show interface brief](#)
[show interface status](#)

show interface status

Overview Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

Syntax `show interface [<port-list>] status`

Parameter	Description
<code><port-list></code>	The ports to display information about. The port list can be: • an Eth port (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth1-eth2) • a comma-separated list (e.g. eth1,eth2). Do not mix interface types in a list.

Mode User Exec and Privileged Exec

Examples To display the status of eth1.2 and eth1.3, use the command:

```
awplus# show interface eth1.2,eth1.3 status
```

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

```
awplus# show interface status
```


Output The following shows typical output.

Example output from the show interface <port-list> status command

```
awplus#show interface eth1.2,eth1.3 status
Port      Name      Status      Vlan Duplex  Speed Type
eth1.2    area2     connected   none a-full a-1000
eth1.3    area3     connected   none a-full a-1000
```

Example output from the show interface status command

```
awplus#show interface status
Port      Name      Status      Vlan Duplex  Speed Type
eth1      eth1      connected   none a-full a-1000 1000BASE-T
eth1.3    area3     connected   none a-full a-1000
eth1.2    area2     connected   none a-full a-1000
...
```

Parameters in the output from the show interface status command

Parameter	Description
Port	Name/Type of the interface.
Name	Description of the interface.
Status	The administrative and operational status of the interface; one of: - disabled: the interface is administratively down. - connect: the interface is operationally up. - notconnect: the interface is operationally down.
Vlan	VLAN type or VLAN IDs associated with the port: When the port is an Eth port, it displays none: there is no VLAN associated with it.
Duplex	The actual duplex mode of the interface, preceded by a- if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.
Speed	The actual link speed of the interface, preceded by a- if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.
Type	The type of interface, e.g. 1000BaseTX.

Related commands [show interface](#)
[show interface brief](#)
[show interface memory](#)

shutdown

Overview This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer. Use the **no** variant of this command to disable this function and bring the link back up again.

Syntax shutdown
no shutdown

Mode Interface Configuration

Example To shut down eth1, use the commands:

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

To bring up eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no shutdown
```

10

Wireless Commands

- Contents**
- **Introduction** on page 395
 - **3gpp-info (wireless-network-passpoint-dot11u)** on page 396
 - **additional-step-required enable (wireless-network-passpoint-dot11u)** on page 397
 - **airtime-fairness mode (wireless-ap-prof-radio)** on page 398
 - **airtime-percentage** on page 400
 - **anqp-domain-id (wireless-network-passpoint-hs20)** on page 402
 - **anqp-element (wireless-network-passpoint-dot11u)** on page 403
 - **antenna (wireless-ap-prof-radio)** on page 404
 - **ap local** on page 405
 - **ap-profile local** on page 406
 - **association-advertisement enable** on page 407
 - **atmf-application-proxy port enable** on page 408
 - **authentication (wireless-sec-wep)** on page 409
 - **auto-discovery disable** on page 410
 - **band-steering (wireless-network)** on page 411
 - **bandwidth (wireless-ap-prof-radio)** on page 412
 - **bcast-key-refresh-interval (wireless-sec-wpa-ent)** on page 413
 - **bcast-key-refresh-interval (wireless-sec-wpa-psnl)** on page 414
 - **bss-trans-manage enable** on page 415
 - **captive-portal** on page 416
 - **captive-portal virtual-ip** on page 417
 - **channels (wireless-ap-prof-radio)** on page 418
 - **channel (wireless-ap-radio)** on page 419
 - **ciphers (wireless-sec-wpa-ent)** on page 420
 - **ciphers (wireless-sec-wpa-psnl)** on page 421
 - **client-isolation-mode** on page 422
 - **conn-capability protocol (wireless-network-passpoint-hs20)** on page 423
 - **country-code** on page 425
 - **deauth-req-timeout (wireless-network-passpoint-hs20)** on page 426
 - **debug wireless** on page 427
 - **description (wireless-ap)** on page 430
 - **description (wireless-ap-prof)** on page 431
 - **description (wireless-mac-ftt)** on page 432
 - **description (wireless-network)** on page 433

- **description (wireless-sc-prof)** on page 434
- **dgaf enable (wireless-network-passpoint-hs20)** on page 435
- **domain-name (wireless-network-passpoint-dot11u)** on page 436
- **dot11u (wireless-network-passpoint)** on page 437
- **dtim-period** on page 438
- **dup-auth-received (wireless-network)** on page 439
- **emergency-service-reachable enable (wireless-network-passpoint-dot11u)** on page 440
- **enable (wireless-ap-prof-radio)** on page 441
- **enable (wireless-network-cp)** on page 442
- **enable (wireless-network-passpoint)** on page 443
- **external-page-url** on page 444
- **force-disable (wireless-ap-radio)** on page 445
- **gas-address-behavior (wireless-network-passpoint-dot11u)** on page 446
- **gas-comeback-delay (wireless-network-passpoint-dot11u)** on page 447
- **hessid (wireless-network-passpoint-dot11u)** on page 448
- **hide-ssid (wireless-network)** on page 450
- **hs20 (wireless-network-passpoint)** on page 451
- **inactivity-timer** on page 452
- **index** on page 453
- **initialization-button enable** on page 454
- **internet-access enable (wireless-network-passpoint-dot11u)** on page 455
- **ip-addr-type-availability (wireless-network-passpoint-dot11u)** on page 456
- **key (wireless-sc-prof)** on page 458
- **key (wireless-sec-wep)** on page 459
- **key (wireless-sec-wpa-psnl)** on page 461
- **l2tif enable (wireless-network-passpoint-hs20)** on page 462
- **led enable** on page 463
- **legacy-rates** on page 464
- **length (wireless-sec-wep)** on page 466
- **mac-auth dynamic-vlan enable** on page 467
- **mac-auth mode** on page 469
- **mac-auth two-step-auth-with-cp enable** on page 470
- **mac-auth password** on page 471
- **mac-auth radius auth group (wireless-network)** on page 472
- **mac-auth radius dynamic-authorization-client** on page 473
- **mac-auth radius send service-type** on page 474
- **mac-auth username** on page 475
- **management-frame-protection enable (wireless-sec-wpa-ent)** on page 477
- **management-frame-protection enable (wireless-sec-wpa-psnl)** on page 479
- **max-clients** on page 481
- **mode (wireless-ap-prof-radio)** on page 482

- **multicast-to-unicast enable** on page 484
- **multicast-tx-rate** on page 485
- **mode (wireless-network-cp)** on page 487
- **nai-realm (wireless-network-passpoint-dot11u)** on page 489
- **neighbor-ap-detection enable** on page 491
- **network-auth-type (wireless-network-passpoint-dot11u)** on page 492
- **network-type (wireless-network-passpoint-dot11u)** on page 494
- **network (wireless)** on page 496
- **operating-class (wireless-network-passpoint-hs20)** on page 497
- **operator (wireless-network-passpoint-hs20)** on page 498
- **page-proxy-url** on page 499
- **passpoint** on page 500
- **power (wireless-ap-radio)** on page 501
- **pre-authentication enable (wireless-sec-wpa-ent)** on page 502
- **proxy-arp enable** on page 503
- **proxy-arp-through enable** on page 504
- **qos-map-set (wireless-network-passpoint-dot11u)** on page 505
- **radio (wireless-ap)** on page 506
- **radio (wireless-ap-profile)** on page 507
- **radius accounting enable** on page 508
- **radius auth group (wireless-network-cp)** on page 509
- **radius auth group (wireless-sec-wpa-ent)** on page 511
- **redirect-url** on page 512
- **roaming-oi (wireless-network-passpoint-dot11u)** on page 513
- **rts-threshold** on page 514
- **rule (wireless-mac-filter)** on page 515
- **sc-profile** on page 516
- **security (wireless)** on page 517
- **security (wireless-network)** on page 519
- **session-keep** on page 520
- **session-key-refresh-action** on page 521
- **session-key-refresh-interval** on page 522
- **session-timeout-action (wireless network-cp)** on page 523
- **session-timeout-interval (wireless network-cp)** on page 524
- **show debugging wireless** on page 525
- **show wireless** on page 526
- **show wireless ap** on page 527
- **show wireless ap capability** on page 529
- **show wireless ap clients** on page 532
- **show wireless ap counter** on page 533
- **show wireless ap neighbors** on page 534
- **show wireless ap-profile** on page 535
- **show wireless captive-portal network walled-garden** on page 537
- **show wireless country-code** on page 538
- **show wireless network** on page 539
- **show wireless security** on page 543

- **show wireless wireless-mac-filter** on page 545
- **single-channel-scan enable** on page 547
- **single-channel-scan duration** on page 548
- **single-channel-scan interval** on page 549
- **single-channel-scan keep-data-time** on page 550
- **smart-connect-profile** on page 551
- **ssid (wireless-network)** on page 552
- **ssid (wireless-sc-prof)** on page 553
- **station-isolation enable (wireless-ap-prof-radio)** on page 554
- **type (wireless-sec-wep)** on page 556
- **unauth-emergency-service-access enable (wireless-network-passpoint-dot11u)** on page 557
- **unassociated-client-list acquire** on page 558
- **vap (wireless-ap-prof-radio)** on page 559
- **versions (wireless-sec-wpa-ent)** on page 560
- **versions (wireless-sec-wpa-psnl)** on page 561
- **vlan (wireless-network)** on page 562
- **walled-garden-dns-proxy enable** on page 563
- **walled-garden entry** on page 564
- **wan-metrics downlink-load (wireless-network-passpoint-hs20)** on page 566
- **wan-metrics downlink-speed (wireless-network-passpoint-hs20)** on page 567
- **wan-metrics info (wireless-network-passpoint-hs20)** on page 568
- **wan-metrics load-measure-duration (wireless-network-passpoint-hs20)** on page 570
- **wan-metrics uplink-load (wireless-network-passpoint-hs20)** on page 571
- **wan-metrics uplink-speed (wireless-network-passpoint-hs20)** on page 572
- **web-auth radius auth group** on page 573
- **wireless** on page 574
- **wireless ap-configuration apply ap local** on page 575
- **wireless ap-configuration pull ap** on page 576
- **wireless disassociate ap local client** on page 577
- **wireless export** on page 578
- **wireless import** on page 579
- **wireless-mac-filter (wireless)** on page 580
- **wireless-mac-filter-id** on page 581
- **wireless-mac-filter (wireless-ap-prof)** on page 583
- **wireless-mac-filter enable** on page 585

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure a wireless router.

For more information, see the [Wireless Management Guide using the Device GUI](#).

3gpp-info (wireless-network-passpoint-dot11u)

Overview Use this command to set the 3GPP (802.11u 3rd Generation Partnership Project) cellular network information.

Use the **no** variant of this command to revert to the default value.

Syntax 3gpp-info <code-list>
no 3gpp-info

Parameter	Description
<code-list>	Enter the MCC (Mobile Country Code) and MNC (Mobile Network Code): • MCC must be a 3 digit decimal number • MNC must be a 2 or 3 digit decimal number • MCC and MNC must be separated by commas • If setting multiple combinations of MCC and MNC, they must be separated by semicolons. • A maximum of 100 characters can be set including commas and semicolons. For more information on mobile country and network codes, go to: Wikipedia Mobile Country Codes.

Default Not set.

Mode Wireless Network Passpoint 802.11u Configuration

Example To set some of the MCC and MNC codes for Japan, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# 3gpp-info
440,00;440,50
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

additional-step-required enable (wireless-network-passpoint-dot11u)

Overview Use this command to configure an Additional Step Required for Access.

Use the **no** variant of this command to disable Additional Step Required for Access.

Syntax additional-step-required enable
no additional-step-required enable

Default Disabled.

Mode Wireless Network Passpoint 802.11u Configuration

Usage notes Typically, access and authentication is automatic if a legacy hotspot is operated by the mobile device's Home Service Provider (SP) or if the user has previously authenticated to that hotspot. Additionally, user intervention is typically required in a roaming environment where the hotspot is not operated by the Home SP and additional steps are required to identify and authenticate with the Home SP.

Example To enable Additional Step Required for Access, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# additional-
step-required enable
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

airtime-fairness mode (wireless-ap-prof-radio)

Overview Use this command to improve network throughput by more fairly distributing airtime between wireless clients. Airtime fairness applies to the transmission channel of your device's radio; it does not affect the transmission channel of clients themselves.

Use the **no** variant of this command to remove the airtime fairness configuration from your device's radio.

Syntax `airtime-fairness mode {evenly|manual}`
`no airtime-fairness [enable]`

Parameter	Description
<code>evenly</code>	Evenly allocate time to all clients connected to the radio regardless of which VAP they have associated with.
<code>manual</code>	Allocate airtime to clients connected to the radio, weighted by the airtime-fairness-percentage configured on each VAP.
<code>enable</code>	For the no variant, enable is an optional parameter that can be included. Airtime fairness will still be disabled if you don't specify this parameter.

Default Disabled.

Mode Wireless AP Profile Radio Configuration

Usage notes Airtime fairness is a feature designed to improve network throughput by distributing airtime more equitably among wireless clients. It works by allocating airtime proportionally to clients based on their data transmission speeds

Client devices running on older wireless standards (such as 802.11a, 802.11g, and 802.11n), due to their lower bandwidth and older protocols, take a longer duration of airtime to transmit a given packet compared to newer standards.

By default, the device's radio operates in round-robin mode, transmitting packets to each client in turn. This means the device spends more time transmitting to older, slower clients, which reduces the time available for faster clients, ultimately lowering overall network throughput.

When airtime fairness is enabled, the device allocates airtime to clients in a round-robin fashion, transmitting as many packets as possible to each client within their allotted time window. This method sends proportionally more packets to faster clients, reducing packets for slower clients, which results in higher overall network throughput.

Example To configure radio 1 to operate in 'evenly' mode for airtime fairness, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# airtime-fairness mode
evenly
```

Related commands [radio \(wireless-ap\)](#)
[airtime-percentage](#)
[show wireless ap-profile](#)

Command changes Version 5.5.4-1.1: command added

airtime-percentage

Overview Use this command to set each VAP's airtime fairness (ATF) percentage manually. This command has no effect unless the related command **airtime-fairness mode manual** is configured on the VAP's radio.

ATF ensures that every client has equal access to air time, regardless of client capability (operating system, 802.11 mode, RSSI). The ATF percentage is configured on wireless networks in the range of 0 to 100, however, the total configured for all networks attached to a radio cannot exceed 100%.

Use the **no** variant of this command to disable airtime-fairness percentage on a VAP's radio.

Syntax `airtime-percentage <1-100>`
`no airtime-percentage`

Parameter	Description
<code><1-100></code>	Percentage of airtime to reserve for this network. All networks attached to a radio must have percentages that total 100% or less.

Default Zero.

Mode Wireless Network Configuration

Example To configure VAP1 on radio 1 with an airtime percentage of 50%, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 3
awplus(config-wireless-network)# airtime-percentage 50
awplus(config-wireless-network)# exit
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# airtime-fairness mode
manual
awplus(config-wireless-ap-prof-radio)# vap 1 network 3
```

To remove the airtime fairness percentage on VAP1 on radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 3
awplus(config-wireless-network)# no airtime-percentage
```

Related commands **network (wireless)**
airtime-fairness mode (wireless-ap-prof-radio)

Command changes Version 5.5.4-1.1: command added

anqp-domain-id (wireless-network-passpoint-hs20)

Overview Use this command to set the ANQP (Access Network Query Protocol) domain identifier.

Use the **no** variant of this command to reset the ANQP domain identifier to the default value.

Syntax `anqp-domain-id <0-65535>`
`no anqp-domain-id`

Parameter	Description
<code><0-65535></code>	ANQP domain identifier.

Default 0

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set the ANQP domain identifier on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# anqp-domain-id 1
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

anqp-element (wireless-network-passpoint-dot11u)

Overview Use this command to configure the Arbitrary Access Network Query Protocol (ANQP) element.

ANQP is a query and response protocol that defines services offered by an access point (AP), typically at a Wi-Fi hot spot.

Use the **no** variant of this command to remove a specified ANQP element entry.

Syntax `anqp-element info-id <0-999> payload HEX`
`no anqp-element info-id <0-999>`

Parameter	Description
<0-999>	Arbitrary ANQP element configuration's unique entry number.
HEX	Arbitrary ANQP element configuration. The maximum number of characters in HEX is 100.

Default Not set.

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure the ANQP element info ID to '1' and the payload HEX value to '0000', use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# anqp-element
info-id 1 payload 0000
```

Related commands [show wireless network dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

antenna (wireless-ap-prof-radio)

Overview Use the antenna command to set the antenna model.
Use the **no** variant of this command to remove the antenna model setting.

Syntax antenna at-tq0301
no antenna

Parameter	Description
an2458-10dp	Antenna model AN2458-10DP
an5158-16dp	Antenna model AN5158-16DP
an5158-19dp	Antenna model AN5158-19DP

Default Not set.

Mode Wireless AP Profile Radio Configuration

Example To configure the antenna model TQ0301, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# antenna at-tq0301
```

Related commands [radio \(wireless-ap-profile\)](#)

Command changes Version 5.4.7-2.4: command added

ap local

Overview Use this command to enter your device's access point (AP) configuration mode. You use this mode to configure your device's AP setting.

Syntax `ap local`

Mode Wireless Configuration

Usage notes Before entering local AP configuration mode, you must first enter Wireless Configuration mode.

Example To enter AP local configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap local
awplus(config-wireless-ap)#
```

Related commands [show wireless](#)

Command changes Version 5.5.3-1.1: command added

ap-profile local

Overview Use this command to enter your device's access point (AP) Profile configuration mode. This mode is for configuring your device's AP Profile.

Syntax `ap-profile local`

Mode Wireless Configuration

Usage notes Before entering local AP Profile configuration mode, you must first enter Wireless Configuration mode.

Example To enter local AP Profile configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)#
```

Related commands [show wireless ap-profile](#)

Command changes Version 5.5.3-1.1: command added

association-advertisement enable

Overview Use this command to enable an Association Advertisement on the network configuration.

Use the **no** variant of this command to disable the Association Advertisement on the network configuration.

Syntax association-advertisement enable
no association-advertisement enable

Default Disabled.

Mode Wireless Network Configuration

Example To enable the Association Advertisement for network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# association-advertisement
enable
```

Related commands [show wireless network](#)
[network \(wireless\)](#)

Command changes Version 5.5.1-0.1: command added

atmf-application-proxy port enable

Overview Use this command to enable AMF Security mini to communicate with the wireless controller. Optionally you can also specify a port number for that communication. This is needed for AMF Security mini to control how clients of TQ series APs access the wireless network.

Use the **no** variant of this command to stop AMF Security mini from communicating with the wireless controller. This also resets the port number to the default.

After entering this command, restart the wireless controller, using the command **no enable** followed by **enable**.

Syntax atmf-application-proxy port enable [<1-65535>]
no atmf-application-proxy port enable

Parameter	Description
<1-65535>	The port number through which AMF Security mini will communicate with the wireless controller.

Default Status: Disabled
Port number: 5443

Mode Wireless Configuration

Usage notes We recommend configuring this feature through the AMF Security mini GUI, rather than through this command.

Example To enable AMF Security mini to communicate with the wireless controller through port 5000, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# atmf-application-proxy port enable 5000
awplus(config-wireless)# no enable
awplus(config-wireless)# enable
```

Related commands [show wireless](#)
[wireless](#)

Command changes Version 5.5.2-2.1: command added

authentication (wireless-sec-wep)

Overview Use this command to enable or disable authentication on a wireless Access Point (AP).

Syntax authentication {both|open-system|shared-key}

Parameter	Description
both	Use both types of authentication: open-system and shared-key authentication.
open-system	No authentication.
shared-key	WEP authentication.

Default Open-system.

Mode Wireless Security WEP Configuration

Usage notes For **MWS** series devices, select either the open-system or shared-key parameter. You can't select the **both** parameter.

Example To configure WEP as the security authentication mode for clients, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 10 mode wep
awplus(config-wireless-sec-wep)# authentication shared-key
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

auto-discovery disable

Overview Use this command to disable the automatic search for new APs in an AWC Smart Connect (AWC-SC) network.

Use the **no** variant of this command to enable the automatic search for new APs.

Syntax auto-discovery disable
no auto-discovery disable

Default Enabled

Mode Wireless Smart Connect Profile Configuration

Usage notes Auto-discovery is a function that allows an AP that is in the factory default state to automatically become part of an AWC-SC network. This is because when a wireless AP is activated in the factory default state, its IP and MAC address are added to the AP profile and the Smart Connect profile.

Example To turn auto-discovery off for Smart Connect profile 10, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# smart-connect-profile 10
awplus(config-wireless-sc-prof)# auto-discovery disable
```

Related commands [smart-connect-profile](#)

Command changes Version 5.5.0-0.1: command added

band-steering (wireless-network)

Overview Use this command to enable band steering on a wireless Access Point (AP).
Use the **no** variant of this command to disable band steering.

Syntax band-steering
no band-steering

Default Disabled.

Mode Wireless Network Configuration

Usage notes Band Steering detects dual-band capable clients and steers them to the 5 GHz frequency. This leaves the more crowded 2.4 GHz band available for legacy clients.

This helps improve end user experience by reducing channel utilization, especially in high density environments

This command is not supported on the **MWS** series products.

Example To enable band steering, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# band-steering
```

Related commands **network (wireless)**
show wireless network

Command changes Version 5.4.7-2.4: command added.

bandwidth (wireless-ap-prof-radio)

Overview Use this command to assign a bandwidth to a radio.
Use the **no** variant of this command to revert to the default bandwidth.

Syntax bandwidth {20|40|80|160}
no bandwidth

Parameter	Description
20	20MHz bandwidth
40	40MHz bandwidth
80	80MHz bandwidth
160	160MHz bandwidth

Default The default bandwidth value varies according to the configured hardware and radio type.

Mode Wireless AP Profile Radio Configuration

Example To assign a 40MHz bandwidth to Radio 2, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# bandwidth 40
```

Related commands [country-code](#)
[radio \(wireless-ap-profile\)](#)

Command changes Version 5.4.7-2.4: command added.

bcast-key-refresh-interval (wireless-sec-wpa-ent)

Overview Use this command to set the refresh interval for the broadcast key used in a WPA-enterprise security configuration.

Use the **no** variant of this command to set the refresh interval for the broadcast key to the default.

Syntax bcast-key-refresh-interval <0-86400>
no bcast-key-refresh-interval

Parameter	Description
<0-86400>	The refresh interval in seconds For the MWS series , the broadcast key refresh rate is <0, 30-3600> seconds.

Default The default refresh interval is 0 seconds.

Mode Wireless Security WPA-enterprise Configuration

Example To set 3600 seconds as the broadcast key refresh interval, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# bcast-key-refresh-interval
3600
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added

bcast-key-refresh-interval (wireless-sec-wpa-psnl)

Overview Use this command to set the refresh interval for a broadcast (group) key used in a WPA-personal security configuration.

Use the **no** variant of this command to set the refresh interval to the default value.

Syntax bcast-key-refresh-interval <0-86400>
no bcast-key-refresh-interval

Parameter	Description
<0-86400>	The broadcast key refresh interval. For the MWS series , the broadcast key refresh rate is <0, 30-3600> seconds.

Default The default value is 0.

Mode Wireless Security WPA-personal Configuration

Example To set the broadcast key refresh interval to 3600 seconds on a WPA-personal security configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 110 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)# bcast-key-refresh-interval
3600
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

bss-trans-manage enable

Overview Use this command to enable Basic Service Set (BSS) Transition Management on a wireless network configuration. The BSS consists of one redistribution point – typically an access point (WAP or AP) interconnecting all associated wireless clients.

Use the **no** variant of this command to disable BSS Transition Management on a wireless network configuration.

Syntax bss-trans-manage enable
no bss-trans-manage enable

Default Disabled.

Mode Wireless Network Configuration

Example To configure enable BSS Transition Management, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# bss-trans-manage enable
```

Related commands [show wireless network](#)
[network \(wireless\)](#)

Command changes Version 5.5.0-2.3: command added

captive-portal

Overview Use this command to add a Captive Portal (web authentication) configuration and enter the Captive Portal configuration mode.

Captive Portal lets wireless clients authenticate themselves or agree to terms and conditions before you grant them Wi-Fi access or external web access.

Use the **no** variant of this command to remove a Captive Portal configuration.

Syntax captive-portal
no captive-portal

Default Captive Portal is not set.

Mode Wireless Network Configuration

Example To enter the Captive Portal configuration mode of network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
```

To reset all the Captive Portal configuration settings of network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# no captive-portal
```

Related commands [enable \(wireless-network-cp\)](#)
[page-proxy-url](#)
[radius auth group \(wireless-network-cp\)](#)
[redirect-url](#)
[session-keep](#)

Command changes Version 5.4.9-1.1: command added

captive-portal virtual-ip

Overview Use this command to configure the virtual IP address on Captive Portal.

Captive Portal lets wireless clients authenticate themselves or agree to terms and conditions before you grant them Wi-Fi access or external web access.

Use the **no** variant of this command to remove the virtual IP address on Captive Portal.

Syntax captive-portal virtual-ip <ip-address>
no captive-portal virtual-ip

Parameter	Description
<ip-address>	The IPv4 address uses the format A.B.C.D

Default Not set.

Mode Wireless AP Profile Configuration

Usage notes Captive Portal uses the AP's management IP address to show an authentication page. To avoid a potential security risk, this command allows you to hide the AP management IP address by providing a virtual IP address for Captive Portal authentication.

Example To configure a virtual IP address for Captive Portal, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# captive-portal virtual-ip
1.1.1.1
```

Related commands

- [show wireless ap-profile](#)
- [captive-portal](#)
- [page-proxy-url](#)
- [radius auth group \(wireless-network-cp\)](#)
- [redirect-url](#)
- [session-keep](#)
- [mode \(wireless-network-cp\)](#)

Command changes Version 5.5.0-1.3: command added

channels (wireless-ap-prof-radio)

Overview Use this command to set the channel that a wireless Access Point (AP) uses when it is set to auto.

Use the **no** variant of this command to return the AP channel to its default.

Syntax channels <1-255>
no channels

Parameter	Description
<1-255>	The channel number.

Default The default channel varies with each type of AP, its country-code, and outdoor settings.

Mode Wireless AP Profile Radio Configuration

Example To set the wireless AP radio channel, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# channels 10
```

Related commands [radio \(wireless-ap-profile\)](#)
[country-code](#)

Command changes Version 5.4.7-2.4: command added.

channel (wireless-ap-radio)

Overview Use this command to configure a channel on an Access Point (AP). You can configure an AP to automatically select a channel or use a fixed channel.

Use the **no** variant of this command to remove any configured channels and return to the default value.

Syntax `channel {auto|<1-255>}`

`no channel`

Parameter	Description
auto	The channel is automatically selected.
<1-255>	A list of fixed channels. The list is determined by the country-code.

Default The default is **auto**.

Mode Wireless AP Radio Configuration

Example To configure a fixed channel for an AP, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap 100
awplus(config-wireless-ap)# radio 2
awplus(config-wireless-ap-radio)# channel 1
```

Related commands [show wireless ap-profile](#)
[country-code](#)

Command changes Version 5.4.7-2.4: command added.

ciphers (wireless-sec-wpa-ent)

Overview Use this command to set the cipher suite(s) used by WPA-personal security configurations. The cipher suites available are: GCMP, CCMP (AES) and TKIP.

Use the **no** variant of this command to set the default cipher suite used by WPA-personal security configurations.

Syntax ciphers <cipher-list>
no ciphers

Parameter	Description
<cipher-list>	The cipher suite(s) to use. The list can contain: • gcmp • ccmp • tkip, or • both ccmp and tkip (in any order).

Default CCMP

Mode Wireless Security WPA-enterprise Configuration

Example To set both CCMP (AES) and TKIP as cipher suites on a security WPA-enterprise configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# ciphers ccma tkip
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added

ciphers (wireless-sec-wpa-psnl)

Overview Use this command to set the cipher suite(s) used by WPA-personal security configurations. The cipher suites available are: CCMP (AES) and TKIP.

Use the **no** variant of this command to set the default cipher suite used by WPA-personal security configurations.

Syntax ciphers <cipher-list>
no ciphers

Parameter	Description
<cipher-list>	The available cipher suite(s) in list format. The list can contain either ccmp or tkip or both and can be in any order.

Default ccmp.

Mode Wireless Security WPA-personal Configuration

Usage notes For MWS series devices, a combination of versions and ciphers are supported as follows:

- versions wpa2 and ciphers ccmp
- versions wpa, wpa2, and ciphers tkip and ccmp

Example To configure WPA-personal to use both CCMP (AES) and TKIP as cipher suites in a security configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 110 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)# ciphers ccmp tkip
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

client-isolation-mode

Overview Use this command to configure the Client Isolation Mode for the wireless network. If 'VAP' is selected as the Client Isolation Mode, it prohibits communication between wireless clients connected to the same wireless network (VAP).

Use the **no** variant of this command to reset the Client Isolation Mode to the default.

Syntax `client-isolation-mode vap`
`no client-isolation-mode`

Parameter	Description
vap	Set Client Isolation Mode 'vap' to the wireless network. Note, the parameter ap is displayed on the CLI but not supported.

Default Disabled

Mode Wireless Network Configuration

Example To set Client Isolation Mode 'vap' to network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# client-isolation-mode vap
```

Related commands [show wireless network](#)
[network \(wireless\)](#)
[show wireless ap-profile](#)

Command changes Version 5.5.3-1.1: command added

conn-capability protocol (wireless-network-passpoint-hs20)

Overview Use this command to specify the protocols supported by the network connection and the corresponding port numbers and whether the port is open or closed.

Use the **no** variant of this command to remove the settings for the specified protocol number.

Syntax conn-capability protocol <0-255> port <0-65535> status [closed|open|unknown]
no conn-capability protocol <0-255>

Parameter	Description
<0-255>	Protocol number, as in the assigned protocol numbers listed at: www.iana.org .
<0-65535>	Port number
closed	Indicates the connection is in closed mode
open	Indicates the connection is in open mode
unknown	Indicates the connection status is unknown

Default Not set.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Usage notes These settings signify the capabilities of the wired network that the AP is connected to. They provide information on the connection status of the most commonly used communication protocols and ports within the hotspot.

The term 'hs20' is shorthand for Hotspot 2.0. Passpoint is the Wi-Fi Alliance's name for the Hotspot 2.0 program.

Example To set the connection capability on port 161 to 'closed' for protocol 17 (UDP), use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# conn-capability
protocol 17 port 161 status closed
```

Related commands **show wireless network**
hs20 (wireless-network-passpoint)

Command changes Version 5.5.0-2.3: command added

country-code

Overview Use this command to set the country code for an AP-profile.

Use the **no** variant of this command to revert back to the default country code for the device's region.

Syntax country code <code>
no country code

Parameter	Description
<code>	A two letter code representing the country. Use the command show wireless country-code to see the full list of country codes available.

Default The default country code is '**jp**' for Japan or '**us**' for other regions.

Mode Wireless AP Profile Configuration

Usage notes Use the command **show wireless country-code** to display a list of valid country codes.

NOTE: ap-profileap-radio

Example To set the country code to 'New Zealand' for your AP, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# country-code nz
```

Related commands **show wireless country-code**
show wireless ap-profile
channel (wireless-ap-radio)
mode (wireless-ap-prof-radio)
bandwidth (wireless-ap-prof-radio)

Command changes Version 5.4.7-2.4: command added

deauth-req-timeout (wireless-network-passpoint-hs20)

Overview Use this command to configure the deauthentication request timeout.

Use the **no** variant of this command to revert the deauthentication timeout time to the default value.

Syntax deauth-req-timeout <0-65535>
no deauth-req-timeout

Parameter	Description
<0-65535>	The timeout, in seconds, for client deauthentication after sending WNM notification frames. WNM notification requests allow the hotspot feature to send clients the URLs of servers that allow the client to access information about how to subscribe to the service, correct connection errors, or extend the current session.

Default 60 seconds.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To configure a deauthentication request timeout of 120 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# deauth-req-timeout 120
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

debug wireless

Overview Use this command to enable wireless debugging. Debugging filters can be based on severity level and module name.

Use the **no** variant of this command to disable all wireless debugging.

Syntax debug wireless level {all|debug|dump|error|info|notice|trace|warning}
debug wireless module {all|apca|apmgr|apreq|clnmgr|cwmcore|rogue|syncscan}
no debug wireless

Parameter	Description
level	Filters logging events by severity level and displays the output by one of the following configured options:
all	All level events
debug	Debug events
dump	Dump events
error	Error conditions
info	Information messages
notice	Normal, but significant conditions
trace	Trace events
warning	Warning conditions
module	Filters logging events by module name and displays the output by one of the following configured options:
all	All module events
apca	Auto power/channel assignment events
apmgr	AP manager events
apreq	HTTP AP request events
clnmgr	Client manager events
cwmcore	CWM core events
rogue	Rogue events
syncscan	Sync scan events

Default Disabled

Mode User Exec

Example To enable debugging of wireless with 'info' level on the 'apca' module, use the command:

```
awplus# debug wireless level info module apca
```

To disable debugging of wireless, use the command:

```
awplus# no debug wireless
```

Related commands [show debugging wireless](#)

Command changes Version 5.5.0-0.1: command added

description (wireless-ap)

Overview Use this command to specify a description to identify an Access Point (AP).

Use the **no** variant of this command to remove the description of an AP.

Syntax `description <description>`
`no description`

Parameter	Description
<code><description></code>	Text to describe an AP.

Default Not set.

Mode Wireless AP Configuration

Example To specify a description for an AP, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap local
awplus(config-wireless-ap)# description MEETING_SPACE
```

Related commands [ap local](#)
[show wireless ap](#)

Command changes Version 5.4.7-2.4: command added.

description (wireless-ap-prof)

Overview Use this command to give the AP profile 'local' a description.
Use the **no** variant of this command to remove the AP profile's description.

Syntax `description <description>`
`no description`

Default Not set.

Mode Wireless AP Profile Configuration

Example To configure the description "PROF10" for AP profile 'local', use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# description PROF10
```

Related commands [show wireless ap-profile](#)

Command changes Version 5.4.7-2.4: command added

description (wireless-mac-flt)

Overview Use this command to set the description of a wireless MAC filter.
Use the **no** variant of this command to remove the description.

Syntax `description <description>`
`no description`

Parameter	Description
<code><description></code>	Text describing the wireless MAC filter.

Default No description set by default.

Mode Wireless MAC Filter Configuration

Example To set the description of MAC filter '20' to 'mywhitelist', use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# wireless-mac-filter 20
awplus(config-wireless-mac-flt)# description mywhitelist
```

To remove the description from MAC filter '20', use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# wireless-mac-filter 20
awplus(config-wireless-mac-flt)# no description
```

Related commands

- [show wireless ap-profile](#)
- [show wireless wireless-mac-filter](#)
- [wireless export](#)
- [wireless import](#)
- [wireless-mac-filter \(wireless\)](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)
- [wireless-mac-filter enable](#)

Command changes Version 5.4.8-2.1: command added

description (wireless-network)

Overview Use this command to set a description for the wireless network.
Use the **no** variant of this command to remove a description for a wireless network.

Syntax `description <description>`
`no description`

Parameter	Description
<code><description></code>	Set a description for a wireless network.

Default Not set.

Mode Wireless Network Configuration

Example To set the description for a wireless network, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# description GUEST_NETWORK
```

Related commands [network \(wireless\)](#)
[show wireless network](#)

Command changes Version 5.4.7-2.4: command added.

description (wireless-sc-prof)

Overview Use this command to configure a descriptive name for a Smart Connect profile.

Use the **no** variant of this command to remove a Smart Connect profile name.

Syntax `description <sc-profile-name>`
`no description`

Parameter	Description
<code><sc-profile-name></code>	The descriptive name given to a Smart Connect profile.

Default Not set

Mode Wireless Smart Connect Profile Configuration

Example To set the descriptive name of SC-PROF10 for Smart Connect profile 10, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# smart-connect-profile 10
awplus(config-wireless-sc-prof)# description SC-PROF10
```

Related commands [smart-connect-profile](#)
[show wireless ap-profile](#)

Command changes Version 5.5.0-0.1: command added

dgaf enable (wireless-network-passpoint-hs20)

Overview Use this command to enable Downstream Group-Addressed Forwarding (DGAF).

Use the **no** variant of this command to disable DGAF.

Syntax dgaf enable
no dgaf enable

Default Enabled.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To disable Downstream Group-Addressed Forwarding on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# no dgaf enable
```

Related commands [show wireless network](#)
[proxy-arp enable](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

domain-name (wireless-network-passpoint-dot11u)

Overview Use this command to configure one or more domain names for the entity operating the AP.

Use the **no** variant of this command to revert to the default value.

Syntax domain-name <domain-name>
no domain-name

Parameter	Description
<domain-name>	The Domain Name(s) • Use the FQDN format, e.g. domain-name example.com • Multiple domain name entries must be separated by a comma • The length of a character in the OI-List must be less than 255 , and 10 elements or less.

Default Not set

Mode Wireless Network Passpoint 802.11u Configuration

Example To set two domain names, mydomain.com and example.net, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# domain-name
mydomain.com, example.net
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

dot11u (wireless-network-passpoint)

Overview Use this command to add a new 802.11u configuration and enter the configuration mode.

Use the **no** variant of this command to revert to the default values.

Syntax dot11u
no dot11u

Default Not set.

Mode Wireless Network Passpoint Configuration

Example To enter the 802.11u configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)#
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)
[passpoint](#)
[network-type \(wireless-network-passpoint-dot11u\)](#)
[hessid \(wireless-network-passpoint-dot11u\)](#)

Command changes Version 5.5.0-2.3: command added

dtim-period

Overview Use this command to set the Delivery Traffic Indication Map (DTIM) period on the network configuration. A DTIM period value is a number that determines how often a beacon frame includes a Delivery Traffic Indication Message, and this number is included in each beacon frame.

Use the **no** variant of this command to reset the DTIM period to the default (1).

Syntax dtim-period <1-5>
no dtim-period

Parameter	Description
<1-5>	DTIM period in seconds. Increasing this number will increase the power saving effect, but it will slow down the response.

Default 1.

Mode Wireless Network Configuration

Usage notes The DTIM is how the AP warns its clients that it is about to transmit the multicast (and broadcast) frames it queued up since the previous DTIM. This queueing and scheduled delivery is done to allow power-conscious devices to save power by turning off their receivers for brief stretches of time, only waking up their receivers when the AP indicates it has traffic for them.

Example To set a DTIM period of 2 seconds on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# dtim-period 2
```

Related commands [show wireless network](#)
[network \(wireless\)](#)

Command changes Version 5.5.1-0.1: command added

dup-auth-received (wireless-network)

Overview Use this command to set a wireless network to accept or ignore 'Duplicate AUTH received' messages. If the message is accepted, then connected clients are disconnected.

Use the **no** variant of this command to use the default action.

Syntax dup-auth-received {disconnect|ignore}
no dup-auth-received

Parameter	Description
disconnect	Accept the disconnect connection request.
ignore	Ignore the disconnection request.

Default Disconnect.

Mode Wireless Network Configuration

Example To configure network 5 to ignore 'Duplicate AUTH received' messages, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 5
awplus(config-wireless-network)# dup-auth-received ignore
```

Related commands [network \(wireless\)](#)
[show wireless ap-profile](#)
[show wireless network](#)

Command changes Version 5.5.1-2.1: command added

emergency-service-reachable enable (wireless-network-passpoint-dot11u)

Overview Use this command to configure Emergency Services Reachable.
Use the **no** variant of this command to disable Emergency Services Reachable.

Syntax emergency-service-reachable enable
no emergency-service-reachable enable

Default Disabled.

Mode Wireless Network Passpoint 802.11u Configuration

Example To enable Emergency Services Reachable, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# emergency-
service-reachable enable
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

enable (wireless-ap-prof-radio)

Overview Use this command to enable a wireless Access Point (AP) profile radio configuration.

Use the **no** variant of this command to disable a wireless AP profile radio configuration.

Syntax enable
no enable

Default Disabled.

Mode Wireless AP Profile Radio Configuration

Example To enable an AP radio profile configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# enable
```

Related commands [radio \(wireless-ap-profile\)](#)

Command changes Version 5.4.7-2.4: command added

enable (wireless-network-cp)

Overview Use this command to enable Captive Portal (web authentication) configuration on the target network.

Use the **no** variant of this command to disable Captive Portal configuration on the target network.

Syntax enable
no enable

Default Disabled

Mode Wireless Network Configuration

Example To enable Captive Portal, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# enable
```

Related commands [page-proxy-url](#)
[redirect-url](#)
[session-keep](#)

Command changes Version 5.4.9-1.1: command added

enable (wireless-network-passpoint)

Overview Use this command to enable Passpoint.
Use the **no** variant of this command to disable Passpoint.

Syntax enable
no enable

Default Disabled

Mode Wireless Network Passpoint Configuration

Example To enable Passpoint for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# enable
```

Related commands [passpoint](#)

Command changes Version 5.5.0-2.3: command added

external-page-url

Overview Use this command to configure the external URL authentication page for Captive Portal.

To use this command, you must first specify external-page-redirect using the **mode** command.

Use the **no** variant of this command to reset the external authentication page URL.

Syntax external-page-url <URL>
no external-page-url

Parameter	Description
<URL>	URL of the external authentication page

Default Disabled

Mode Wireless Network Captive Portal Configuration

Example To enable and set URL string 'http://www.example.com' for a Captive Portal external web authentication server on network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# external-page-url http://
www.example.com
```

Related commands [captive-portal virtual-ip](#)
[mode \(wireless-network-cp\)](#)
[radius auth group \(wireless-network-cp\)](#)
[show wireless network](#)

Command changes Version 5.5.0-1.3: command added

force-disable (wireless-ap-radio)

Overview Use this command to override and force the disabling of an Access Point (AP) radio status.

Use the **no** variant of this command to stop overrides of an AP radio status.

Syntax force-disable
no force-disable

Default **no force-disable** (do not override the AP profile radio status).

Mode Wireless AP Radio Configuration

Example To force a disable of an AP radio status, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap 100
awplus(config-wireless-ap)# radio 2
awplus(config-wireless-ap-radio)# force-disable
```

Related commands [show wireless ap-profile](#)
[radio \(wireless-ap-profile\)](#)

Command changes Version 5.4.7-2.4: command added

gas-address-behavior (wireless-network-passpoint-dot11u)

Overview Use this command to set the GAS (Generic Advertisement Services) Address 3 behavior for 802.11u.

Use the **no** variant of this command to revert to the default value.

Syntax gas-address-behavior <0-2>
no gas-address-behavior

Parameter	Description
<0-2>	GAS Address 3 behavior. • 0: P2P specification (Address3 = AP BSSID) workaround enabled by default based on GAS request Address3. • 1: IEEE 802.11 standard compliant regardless of GAS request Address3 • 2: Force non-compliant behavior (Address3 = AP BSSID for all cases)

Default 0.

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure the GAS Address 3 behavior value to 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# gas-address-behavior 1
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

gas-comeback-delay (wireless-network-passpoint-dot11u)

Overview Use this command to set the generic advertisement service (GAS) comeback-delay for 802.11u.

Use the **no** variant of this command to revert to the default value.

Syntax gas-comeback-delay <0-65535>
no gas-comeback-delay <0-65535>

Parameter	Description
<0-65535>	GAS comeback delay Time Unit (TU) 1 TU = 1024 microseconds (approx 1 millisecond)

Default 0.

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure the GAS comeback-delay value to 100, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# gas-comeback-delay 100
```

Related commands [show wireless network dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

hessid (wireless-network-passpoint-dot11u)

Overview Use this command to set the HESSID (Homogeneous Extended Service Set Identifier).

Use the **no** variant of this command to revert to the default value.

Syntax hessid MAC
no hessid

Parameter	Description
MAC	Homogeneous ESS Identifier, in Hexidecimal notation and MAC address format: HHHH.HHHH.HHHH.HHHH

Default Not set.

Mode Wireless Network Passpoint 802.11u Configuration

Usage notes In typical Wi-Fi deployments, if two APs have different SSIDs, they are considered to be in different wireless networks.

If two APs have the same SSID, they are considered to be part of the same wireless network. But because SSIDs are not globally administered, it is possible that two APs with the same SSID are, in fact, in different wireless networks.

The homogeneous extended service set identifier (HESSID) element allows mobile devices to detect this condition. When two APs have the same SSID but from different wireless networks, the two networks have different HESSIDs

Example To set the Homogeneous ESS Identifier '02AA.BBCC.1122', use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# hssid
02AA.BBCC.1122
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

hide-ssid (wireless-network)

Overview Use this command to hide the SSID for a selected wireless network.

Use the **no** variant of this command to stop hiding the SSID for a selected wireless network.

Syntax hide ssid
no hide ssid

Default The default is Disabled, which means the SSID **is** included in the Access Point (AP) beacon frames. For more information, see the **Usage** section below.

Mode Wireless Network Configuration

Usage notes The SSID differentiates one wireless network from another, so all APs and all devices attempting to connect to a specific wireless network must use the same SSID to enable effective roaming.

SSIDs are included in beacon frames.

A beacon frame is one of the management frames in the IEEE 802.11 standard. Every compliant AP periodically sends beacon frames to advertise the presence of an AP in an area, its capabilities, and some configuration and security information to the client devices.

Example To hide the SSID for network 20, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# hide-ssid
```

Related commands [ssid \(wireless-network\)](#)
[network \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

hs20 (wireless-network-passpoint)

Overview Use this command to add a new Hotspot 2.0 configuration and enter the configuration mode.

Use the **no** variant of this command to revert to the default.

Syntax hs20
no hs20

Default Not set.

Mode Wireless Network Passpoint Configuration

Example To enter Hotspot 2.0 configuration mode on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)#
```

Related commands **show wireless network**
passpoint
dgaf enable (wireless-network-passpoint-hs20)
l2tif enable (wireless-network-passpoint-hs20)
operator (wireless-network-passpoint-hs20)
anqp-domain-id (wireless-network-passpoint-hs20)
deauth-req-timeout (wireless-network-passpoint-hs20)
operating-class (wireless-network-passpoint-hs20)

Command changes Version 5.5.0-2.3: command added

inactivity-timer

Overview Use this command to set the inactivity timer on a wireless network. This means that APs in the specified wireless network will disconnect clients who are no longer responding after the configured inactivity time.

Use the **no** variant of this command to reset the inactivity timer to the default.

Syntax `inactivity-timer <30-3600>`
`no inactivity-timer`

Parameter	Description
<code><30-3600></code>	Time in seconds

Default 300 seconds.

Mode Wireless Network Configuration

Example To set an inactivity timer of 600 seconds on network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# inactivity-timer 600
```

To reset the inactivity timer to the default, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# no inactivity-timer
```

Related commands [show wireless network](#)
[network \(wireless\)](#)

Command changes Version 5.5.3-1.1: command added

index

Overview Use this command to designate the key index number for WEP security.
Use the **no** variant of this command to use the default key index number for WEP security.

Syntax index <1-4>
no index

Parameter	Description
<1-4>	The index number for the WEP security key.

Default The default key index number is set to **1**.

Mode Wireless Security WEP Configuration

Example To assign key index number 3 for a WEP security configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10 mode wep
awplus(config-wireless-sec-wep)# index 3
```

Related commands [security \(wireless\)](#)
[key \(wireless-sec-wep\)](#)

Command changes Version 5.4.7-2.4: command added.

initialization-button enable

Overview Use this command to enable the initialization (reset) button on the device.
Use the **no** variant of this command to disable the initialization (reset) button on the device.

Syntax initialization-button enable
no initialization-button enable

Default Enabled.

Mode Wireless AP Profile Configuration

Usage notes This command effects only APs which have an initialization button.

Example To enable the initialization button, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# initialization-button enable
```

Related commands [show wireless ap-profile](#)

Command changes Version 5.4.7-2.4: command added.

internet-access enable (wireless-network-passpoint-dot11u)

Overview Use this command to enable Internet access. This informs the mobile device whether Internet access is available at a hotspot – which might not be the case in walled-garden environments, where the Hotspot Operator (for example, an hotel) may limit Wi-Fi access to locally available content.

Use the **no** variant of this command to disable Internet access.

Syntax internet-access enable
no internet-access enable

Default Disabled.

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure Internet access, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# internet-
access enable
```

Related commands [show wireless network dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

ip-addr-type-availability (wireless-network-passpoint-dot11u)

Overview Use this command to set the IPv4 and IPv6 Address Type Availability for 802.11u.

This is information about the IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network.

Use the **no** variant of this command to reset the IPv4 and IPv6 Address Type Availability to their default value.

Syntax ip-addr-type-availability {no-exist|public|port-restrict|private-nat1|private-nat2|port-private-nat1|port-private-nat2|unknown} ipv4 {no-exist|exist|unknown}
no ip-addr-type-availability

Parameter	Description
no-exist (ipv4)	Not exist IPv4.
public (ipv4)	Public IPv4.
port-restrict (ipv4)	IPv4 with port restrictions.
private-nat1 (ipv4)	Private IPv4 address with Network Address Translation (NAT) once.
private-nat2 (ipv4)	Private IPv4 address with Network Address Translation (NAT) twice.
port-private-nat1 (ipv4)	Private IPv4 with port restrictions and Network Address Translation (NAT) once.
port-private-nat2 (ipv4)	Private IPv4 with port restrictions and Network Address Translation (NAT) twice.
unknown (ipv4)	Availability unknown IPv4
no-exist (ipv6)	Not exist IPv6
exist (ipv6)	Exist IPv6
unknown (ipv6)	Availability unknown IPv6

Default IPv4: port-private-nat1.

IPv6: no-exist

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure the IPv4 Address Type Availability to public and the IPv6 to no-exist, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# ip-addr-type-availability public ipv6 no-exist
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

key (wireless-sc-prof)

Overview Use this command to set the Smart Connect profile security key.
Use the **no** variant of this command to remove the security key from the Smart Connect profile.

Syntax key <key-word>
no key

Parameter	Description
<key-word>	The WPA shared key. This is an alphanumeric string 8-64 characters long.

Default Not set

Mode Wireless Smart Connect Profile Configuration

Usage notes This command configures the WPA shared key for the Smart Connect network. If no key is set, the security key will be automatically generated.

Example To set the security key for Smart Connect profile 10 to 'sc10-secret-keyword', use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# smart-connect-profile 10
awplus(config-wireless-sc-prof)# key sc10-secret-keyword
```

Related commands [smart-connect-profile](#)
[show wireless ap-profile](#)

Command changes Version 5.5.0-0.1: command added

key (wireless-sec-wep)

Overview Use this command to set the key-string for a WEP security configuration.

Use the **no** variant of this command to remove a key-string for a WEP security configuration.

Syntax key <1-4> [encrypted] <key-string>
no key <1-4>

Parameter	Description
<1-4>	The key's index number. To configure the index number(s), use the index command.
encrypted	This parameter is displayed in show running-config output to indicate that it is displaying the password in encrypted form. You should not enter encrypted on the CLI yourself.
<key-string>	The usable key-string characters, which depend on the key-string type. Use the type command to configure the key-string character type. See the table in the usage section below for more information.

Default Not set.

Mode Wireless Security WEP Configuration

Usage notes When using the **key** command, also use the **type** command to set the key-string type to either ASCII or Hex, this will also set the character and bit number limits as follows.

Type	Number of bits	Number of characters	Case sensitive
ascii	64	5	Yes
ascii	128	13	Yes
hex	64	10	No
hex	128	26	No

Example To assign the word 'friend' as the key-string at index 3 for a WEP security configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 10 mode wep
awplus(config-wireless-sec-wep)# type ascii
awplus(config-wireless-sec-wep)# key 3 friend
```

Related commands **type (wireless-sec-wep)**
length (wireless-sec-wep)
index

Command changes Version 5.4.7-2.4: command added.

key (wireless-sec-wpa-psnl)

Overview Use this command to set a string as the shared secret key on a wireless security WPA-personal configuration.

Use the **no** variant of this command to reset the shared key to the default.

Syntax key [encrypted] <key-string>
no key

Parameter	Description
encrypted	This parameter is displayed in show running-config output to indicate that it is displaying the password in encrypted form. You should not enter encrypted on the CLI yourself.
<key-string>	The usable key-string characters for the configuration. You can enter 8 to 63 ASCII characters which are case-sensitive.

Default Not set.

Mode Wireless Security WPA-personal Configuration

Example To set **friend** as the shared secret key for a WPA-personal configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 110 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)# key friend
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

l2tif enable (wireless-network-passpoint-hs20)

Overview Use this command to enable Layer 2 Traffic Inspection and Filtering (l2tif).
Use the **no** variant of this command to disable Layer 2 Traffic Inspection and Filtering.

Syntax l2tif enable
no l2tif enable

Default Disabled.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To enable Layer 2 Traffic Inspection and Filtering on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# l2tif enable
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

led enable

Overview Use this command to set the LED color of the PoE port on a wireless router. Use the **no** variant of this command to disable the LED of a wireless AP using the selected AP profile.

Syntax led enable poe-color {amber|green}
no led enable

Parameter	Description
amber	Set the LED color of the PoE port to amber. This is the default color for wireless routers.
green	Set the LED color of the PoE port to green.

Default Enabled, and the LED color is set to amber.

Mode Wireless AP Profile Configuration

Example To set the LED color of the PoE port to green on the wireless router (which uses the local AP profile), use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# led enable poe-color green
```

Related commands [show wireless ap-profile](#)

Command changes Version 5.4.7-2.4: command added

legacy-rates

Overview Use this command to set the legacy rates on the AP profile radio configuration.

Use the **no** variant of this command to delete any configured fixed legacy rates and return to the default.

Syntax legacy-rates {all|<rates>}

no legacy-rates

Parameter	Description
all	All available rate candidates are set for the specified radio.
<rates>	Multiple usable rate candidates can be set on the specified radio, separated by commas. For 2.4 GHz radios: • Select from: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1. • If the bandwidth is 20MHz, you do not have to specify a rate. If you do not specify a rate, the device will use the lowest selected legacy rate as the basic rate. Note that the beacon frame and management frame must use this lowest rate. • If the bandwidth is 40MHz, then 1 must be specified For 5 GHz radios: • Select from: 54, 48, 36, 24, 18, 12, 9, 6. • Regardless of bandwidth, one of 6, 12, or 24 must be specified. Legacy rates do not apply to the 6 GHz radio.

Default All.

Mode Wireless AP Profile Radio Configuration

Example To set specific legacy rates on an AP profile radio configuration, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# legacy-rates
54, 48, 5.5, 2, 1
```

Related commands [show wireless ap-profile](#)
[legacy-rates](#)
[radio \(wireless-ap-profile\)](#)
[bandwidth \(wireless-ap-prof-radio\)](#)

Command changes Version 5.5.4-2.3: removed requirement to specify a rate on Radio 1
Version 5.5.1-0.1: command added

length (wireless-sec-wep)

Overview Use this command to set the key length for a WEP key on a wireless security WEP configuration.

Use the **no** variant of this command to reset the key length for a WEP key to the default value.

Syntax length {64|128}
no length

Parameter	Description
64	Set 64 bit as the key length for a WEP key
128	Set 128 bit as the key length for a WEP key

Default 128 bit.

Mode Wireless Security WEP Configuration

Example To configure 64 bit length as the key length for a WEP key on a wireless security WEP configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10 mode wep
awplus(config-wireless-sec-wep)# length 64
```

Related commands [security \(wireless\)](#)
[key \(wireless-sec-wep\)](#)

Command changes Version 5.4.7-2.4: command added.

mac-auth dynamic-vlan enable

Overview Use this command to set MAC authentication with dynamic VLAN on a wireless network.

Dynamic VLAN lets the wireless router dynamically assign the VLAN into which a device's traffic will be classified, once that device has been authenticated. This is achieved by a collaboration between the authenticator (the wireless router) and the authentication server (the RADIUS server). When the RADIUS server sends back a RADIUS accept message to the authenticator, it can also include attributes in that message that identify a VLAN to which the authenticated device should be assigned.

Use the **no** variant of this command to disable MAC authentication with dynamic VLAN.

Syntax `mac-auth dynamic-vlan enable`
`no mac-auth dynamic-vlan enable`

Default Disabled

Mode Wireless Network Configuration

Usage notes If this feature is enabled on a VAP, you can use dynamic VLAN with MAC authentication by using internal or external RADIUS server for MAC access control. The VLAN ID assigned to the client is determined by the information contained in the Access-Accept message received as part of MAC authentication.

Example To configure MAC authentication with dynamic VLAN for network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth dynamic-vlan enable
```

To disable MAC authentication with dynamic VLAN for network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# no mac-auth dynamic-vlan
enable
```

Related commands [show wireless network](#)

Command changes Version 5.5.4-2.3: command added

mac-auth mode

Overview Use this command to choose the MAC address authentication mode for a wireless network. You can choose to authenticate clients through RADIUS or through AMF Security mini.

Use the **no** variant of this command to reset to no MAC address authentication mode.

Syntax `mac-auth mode {atmf-application-proxy|radius|mac-filter-and-radius}`
`no mac-auth mode`

Parameter	Description
atmf-application-proxy	Use AMF Security mini to authenticate clients.
radius	Use RADIUS to authenticate clients.
mac-filter-and-radius	Use RADIUS and MAC address list filters to authenticate clients.

Default No mode

Mode Wireless Network Configuration

Usage notes We recommend configuring this feature through the AMF Security mini GUI, rather than through this command.

Example To authenticate clients through AMF Security mini on network 10, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10
awplus(config-wireless-network)# mac-auth mode atmf-application-proxy
```

Related commands [atmf-application-proxy port enable](#)
[show wireless network](#)
[wireless](#)

Command changes Version 5.5.5-1.1: default changed to "no mode"
Version 5.5.4-0.1: added **mac-filter-and-radius** parameter for TQ-R series
Version 5.5.2-2.1: command added

mac-auth two-step-auth-with-cp enable

Overview Use this command to configure two-step authentication.

When enabled, STAs (stations) must pass both MAC and Captive Portal (CP) authentication before gaining access (logical **AND** condition).

Use the **no** variant of this command to disable two-step authentication. This allows STAs to pass either MAC **or** CP authentication (logical **OR** condition), rather than requiring both.

Syntax `mac-auth two-step-auth-with-cp enable`
`no mac-auth two-step-auth-with-cp enable`

Default Enabled.

Mode Wireless Network Configuration

Example To enable two-step authentication on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth two-step-auth-with-cp
enable
```

Related commands [show wireless network](#)
[mac-auth mode](#)

Command changes Version 5.5.5-0.1: command added

mac-auth password

Overview Use this command to change the password for MAC-based authentication. Use the **no** variant of this command to return the password to its default.

Syntax `mac-auth password <password>`
`no mac-auth password`

Parameter	Description
<code><password></code>	The new password. Passwords can be up to 64 characters in length and can contain any printable characters except ?, " (double quotes), and spaces.

Default By default the password is the MAC address of the supplicant.

Mode Wireless Network Configuration

Example To set the password for MAC authentication to be 'SECRET', use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# mac-auth password SECRET
```

To reset the password for MAC authentication to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# no mac-auth password
```

Related commands [enable \(wireless-network-cp\)](#)
[network \(wireless\)](#)
[mac-auth radius auth group \(wireless-network\)](#)
[mac-auth username](#)

Command changes Version 5.4.9-2.1: command added

mac-auth radius auth group (wireless-network)

Overview Use this command to enable MAC authentication of clients with a RADIUS group in a wireless network.

Use the **no** variant of this command to disable MAC authentication with a RADIUS group.

Syntax mac-auth radius auth group {radius|<group-name>}
no mac-auth radius auth group

Parameter	Description
radius	Use a RADIUS group, which means all RADIUS servers.
<group-name>	The RADIUS server group.

Default Not set.

Mode Wireless Network.

Usage notes This command enables MAC authentication and designates a RADIUS server group to authenticate clients on a wireless network. RADIUS server groups are defined using the **aaa group server** command. RADIUS server groups can consist of multiple server hosts, but this command only uses two servers.

Example To enable MAC authentication with a RADIUS server group, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10
awplus(config-wireless-network)# mac-auth radius auth group
radius
```

Related commands [network \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

mac-auth radius dynamic-authorization-client

Overview Use this command to configure a Dynamic Authorization Client (DAC) to receive Dynamic Authorization (DA) messages.

Use the **no** variant of this command to remove a Dynamic Authorization Client.

Syntax `mac-auth radius dynamic-authorization-client <ip-address> key <key-string> [encrypted]`
`no mac-auth radius dynamic-authorization-client`

Parameter	Description
<code><ip-address></code>	The client's IPv4 address entered in the form A.B.C.D.
<code>key</code>	Set the client's shared secret key.
<code><key-string></code>	The client's shared secret key in plain text. You can use any printable ASCII characters, but you cannot use quote marks " ", question marks ?, or spaces.
<code>encrypted</code>	This parameter is displayed in show running-config output to indicate that it is displaying the password in encrypted form. You should not enter 'encrypted' on the CLI yourself.

Mode Wireless Network Configuration

Example To configure a DAC to receive DA messages, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth radius dynamic-
authorization-client 192.168.1.1 key testkey
```

Related commands [show wireless network](#)
[mac-auth radius auth group \(wireless-network\)](#)
[mac-auth mode](#)
[stoat discovery](#)
[stoat destination](#)

Command changes Version 5.5.4-0.3: command added

mac-auth radius send service-type

Overview Use this command to enable network devices to send the 'Service-Type' attribute to the RADIUS server during authentication.

By including the Service-Type attribute with a value of 'Call-Check (10)' in the Access-Request, the network device indicates to the RADIUS server that the request is for a call check type of authentication. This can be part of either MAC Authentication RADIUS or WPA-Enterprise authentication modes.

Use the **no** variant of this command to disable devices from sending the 'Service-Type' attribute to the RADIUS server.

Syntax mac-auth radius send service-type
no mac-auth radius send service-type

Default Disabled.

Mode Wireless Network Configuration

Example To send the Service-Type attribute to the RADIUS server on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth radius send service-type
```

Related commands

- [show wireless network](#)
- [mac-auth radius auth group \(wireless-network\)](#)
- [stoat discovery](#)
- [mac-auth mode](#)
- [stoat destination](#)
- [unassociated-client-list acquire](#)

Command changes Version 5.5.4-0.3: command added

mac-auth username

Overview Use this command to set the format of the MAC address in the username and password field when a request for MAC-based authorization is sent to a RADIUS server.

Use the **no** variant of this command to reset the format to the default of hyphen and lower-case.

Syntax `mac-auth username {hyphen|colon|unformatted} {lower-case|upper-case}`

`no mac-auth username`

Parameter	Description
hyphen	The MAC address includes hyphens, e.g. xx-xx-xx-xx-xx-xx.
colon	The MAC address includes colons, e.g. xx:xx:xx:xx:xx:xx.
unformatted	The MAC address does not include hyphens or colons, e.g. xxxxxxxxxxxx.
lower - case	The MAC address uses lower-case characters (a-f).
upper - case	The MAC address uses upper-case characters (A-F).

Default Default format is hyphen lower-case.

Mode Wireless Network Configuration

Example To configure the format of the MAC address in the username and password field to be colon and upper-case, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# mac-auth username colon upper-case
```

To reset the format of the MAC address in the username and password field to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# no mac-auth username
```

Related commands **enable (wireless-network-cp)**
 mac-auth password
 mac-auth radius auth group (wireless-network)
 network (wireless)

Command changes Version 5.4.9-2.1: command added

management-frame-protection enable (wireless-sec-wpa-ent)

Overview Use this command to enable management frame protection (MFP) in a WPA-enterprise configuration.

MFP provides security for management messages passed between wireless Access Points (APs) and client stations. MFP checks management messages for potential security issues such as rogue devices and denial-of-service attacks.

Use the **no** variant of this command to disable MFP.

Syntax management-frame-protection enable [type{capable|required}]
no management-frame-protection enable

Parameter	Description
type	The type of protection, select capable or required . If protection type is omitted, then capable is the default protection type.
capable	Mixed operation. Allows legacy devices that do not support 802.11w to associate while also allowing devices that support 802.11w to use the 802.11w features.
required	Prevents clients that do not support 802.11w from associating with the SSID.

Default Enabled.

Mode Wireless Security WPA-enterprise Configuration

Usage notes Select the protection **type** based on the WPA version:

If the WPA version is:

- a combination of **wpa** and **wpa2**, then protection is disabled
- only **wpa2**, then the protection type can be either **capable**, **required**, or **disabled**
- only **wpa3**, then the protection type is **required**

Example To **disable** MFP, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 110 mode wpa-enterprise
awplus(config-wireless-sec-wpa-psnl)# no management-frame-
protection enable
```

Related commands [security \(wireless\)](#)
[versions \(wireless-sec-wpa-ent\)](#)
[show wireless security](#)

Command changes Version 5.4.7-2.4: command added.
Version 5.5.0-2.3: parameter **type** added

management-frame-protection enable (wireless-sec-wpa-psnl)

Overview Use this command to enable Management Frame Protection (MFP). MFP provides security for management messages passed between wireless Access Points (APs) and client stations. MFP checks management messages for potential security issues such as rogue devices and denial-of-service attacks.

This parameter will be ignored when the version list includes **wpa3** as WPA3 requires that MFP is enabled, see [versions \(wireless-sec-wpa-psnl\)](#).

Use the **no** variant of this command to disable MFP.

Syntax management-frame-protection enable[type{capable|required}]
no management-frame-protection enable

Parameter	Description
type	The type of protection, select capable or required . If protection type is omitted, then capable is the default protection type.
capable	Mixed operation. Allows legacy devices that do not support 802.11w to associate while also allowing devices that support 802.11w to use the 802.11w features.
required	Prevents clients that do not support 802.11w from associating with the SSID.

Default Enabled.

Mode Wireless Security WPA-personal Configuration

Usage notes Select the protection **type** based on the WPA version:

If the WPA version is:

- a combination of **wpa** and **wpa2**, then protection is disabled
- only **wpa2**, then the protection type can be either **capable**, **required**, or **disabled**
- only **wpa3**, then the protection type is **required**

Example To disable MFP, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 100 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)# no management-frame-
protection enable
```

Related commands [security \(wireless\)](#)
[versions \(wireless-sec-wpa-ent\)](#)
[show wireless security](#)

Command changes Version 5.4.7-2.4: command added.
Version 5.5.0-2.3: parameter **type** added

max-clients

Overview Use this command to set the number of wireless clients able to simultaneously connect to the wireless router.

Use the **no** variant of this command to return the number of clients able to connect to the default value.

Syntax max-clients <0-500>
no max-clients

Parameter	Description
<0-500>	The number of clients able to connect to the wireless router. Set this to 0 to stop any clients from connecting to the wireless router.

Default 500.

Mode Wireless AP Profile Radio Configuration

Example To set the maximum number of simultaneous clients that can connect to the wireless router to 128, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# enable
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# max-clients 128
```

Related commands [ap-profile local](#)
[radio \(wireless-ap-profile\)](#)
[show wireless ap-profile](#)

Command changes Version 5.4.7-2.4: command added.

mode (wireless-ap-prof-radio)

Overview Use this command to set the **wireless standard** and **bandwidth** mode used by the Access Points (APs) in a secure wireless security configuration. The AP type or model determines which mode to select.

Use the **no** variant of this command to set the mode to the default values specified for an AP type.

Syntax mode {a|bg|a-n|bg-n|n-only-a|n-only-g|a-n-ac|n-ac|bg-n-ax|a-n-ac-ax|ax}
no mode

Parameter	Standard	Description
a	802.11a	Bandwidth 54Mbps - 5GHz
bg	802.11bg	Bandwidths 11 and 54Mbps- 2.4GHz.
a-n	802.11a/n	Bandwidths 54 and 300 Mbps - 2.4GHz.
bg-n	802.11b/g/n	Bandwidths 11, 54, and 300 Mbps - 2.4GHz
n-only-a	802.11n	Bandwidth 300 Mbps using the 5GHz bandwidth
n-only-g	802.11n	Bandwidth 300 Mbps using the 2.4GHz bandwidth
a-n-ac	802.11a/n/ac	Dual-band: supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands.802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.
n-ac	802.11n/ac	Dual-band: Bandwidth 54, and 300Mbps using both the 2.4 and 5GHz frequencies.
bg-n-ax	802.11b/n/ax	2.4GHz
a-n-ac-ax	802.11b/n/ax	5GHz
ax	802.11ax	6GHz

Default The default values change with each antenna type and AP.

Mode Wireless AP Profile Radio Configuration

Example To configure the wireless mode **a-n-ac** for AP profile local, radio 2, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# mode a-n-ac
```

Related commands **country-code**
radio (wireless-ap-profile)

Command changes Version 5.4.7-2.4: command added.

multicast-to-unicast enable

Overview Use this command to set multicast-to-unicast conversion to a wireless network. When this feature is enabled on the VAP, it converts multicast packet into unicast packets destined for the STA connected to that VAP.

NOTE: *This command is only supported on TQ Router products.*

Use the **no** variant of this command to disable multicast-to-unicast on a specified wireless network.

Syntax multicast-to-unicast enable
no multicast-to-unicast enable

Default Disabled.

Mode Wireless Network Configuration

Example To enable multicast-to-unicast conversion on network 1 of the TQ Router, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# multicast-to-unicast enable
```

To disable multicast-to-unicast conversion on network 1 of the TQ Router, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# no multicast-to-unicast enable
```

Related commands [show wireless network](#)

Command changes Version 5.5.4-1.1: command added

multicast-tx-rate

Overview Use this command to set the multicast transmit (Tx) rate on an AP Profile configuration, in Mbps. This sets the maximum amount of multicast packets the radio can transmit per second.

This command is only supported on wireless routers.

Use the **no** variant of this command to reset the multicast transmit rate to the radio's default value.

Syntax multicast-tx-rate {1|2|5.5|11|12|18|24|36|48|54}
no multicast-tx-rate

Default 11 for Radio 1
6 for Radio 2 and 3

Mode Wireless AP Profile Radio Configuration

Usage notes The following rates are valid for each radio:

- **Radio 1:** 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
- **Radio 2 and 3:** 6, 12, 24

Example To set the multicast transmit rate 12Mbps on Radio 2 of AP Profile local, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# multicast-tx-rate 12
```

To reset the multicast transmit rate on Radio 2 for AP Profile local, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# no multicast-tx-rate
```

Related commands [ap-profile local](#)
[show wireless ap-profile](#)

Command changes Version 5.5.4-2.3: 18, 36, 48 and 54 added
Version 5.5.3-1.1: command added

mode (wireless-network-cp)

Overview Use this command to set the Captive Portal (web authentication) mode. Captive Portal lets wireless clients authenticate themselves or agree to terms and conditions before you grant them Wi-Fi access or external web access.

Use the **no** variant of this command to reset the Captive Portal mode to default.

Syntax mode {click-through|radius|external-page-redirect}
no mode

Parameter	Description
radius	The user name and password entered from the browser screen are sent to the RADIUS server and a network connection is permitted after successful authentication.
click-through	This method asks users to agree to the terms of use (click-through agreement) before allowing them to connect to the wireless network.
external-page-redirect	Redirect the authentication page to a user configured URL such as a third party Captive Portal vendor page.

Default click-through

Mode Wireless Network Captive Portal Configuration

Example To set the Captive Portal authentication mode as RADIUS, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# mode radius
```

Related commands **captive-portal**
enable (wireless-network-cp)
mac-auth password
mac-auth username
page-proxy-url
redirect-url
session-keep

Command changes Version 5.4.9-1.1: command added
Version 5.5.0-1.3: **external-page-redirect** parameter added

nai-realm (wireless-network-passpoint-dot11u)

Overview Use this command to set the NAI (Network Access Identifier) Realm information.

Use the **no** variant of this command to remove a specified NAI Realm entry.

Syntax `nai-realm <realm-number> realm-name <realm-name> eap-method <eap-method>`
`no nai-realm <realm-number>`

Parameter	Description
<code><realm-number></code>	NAI Realm information's unique entry number in the range <1-10>
<code><realm-name></code>	NAI Realm name: • The NAI Realm Name in FQDN (Fully Qualified Domain Name) format. • Multiple NAI Realm Names must be separated by a comma. • The maximum number of characters allowed including commas is 100.
<code><eap-method></code>	Designated EAP method(s) in a list format. The list can use either eap-tls or eap-ttls or eap-sim or two of these three in any order.

Default Not set.

Mode Wireless Network Passpoint 802.11u Configuration

Usage notes A network access identifier (NAI) is a standardized (RFC 4282) format for identifying users requesting access to a network (e.g.user@realm.com). Thus, an NAI Realm identifies the proper authentication server or domain for the user's authentication exchange.

Example To configure an NAI Realm Name and EAP method(s), use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# nai-realm 2
realm-name example.com eap-method eap-tls eap-ttls
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

neighbor-ap-detection enable

Overview Use this command to enable Neighbor AP Detection on the AP profile radio configuration.

Use the **no** variant of this command to disable Neighbor AP Detection for an AP profile radio configuration.

Syntax neighbor-ap-detection enable
no neighbor-ap-detection enable

Default Disabled.

Mode Wireless AP Profile Radio Configuration

Example To enable Neighbor AP Detection for the local AP profile, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# neighbor-ap-detection
enable
```

Related commands [show wireless ap-profile](#)
[radio \(wireless-ap-profile\)](#)

Command changes Version 5.5.1-0.1: command added

network-auth-type (wireless-network-passpoint-dot11u)

Overview Use this command to set the network authentication type.

Use the **no** variant of this command to remove the specified network authentication type.

Syntax network-auth-type {online-enrollment|terms-and-conditions|
redirect-http-https|
redirect-dns} [redirect-url <url>]

no network-auth-type {online-enrollment|terms-and-conditions|
redirect-http-https|
redirect-dns}

Parameter	Description
online-enrollment	Authentication type as online enrollment.
terms-and-conditions	Authentication type as terms and conditions.
redirect-http-https	Redirect using HTTP/HTTPS.
redirect-dns	Redirect using DNS.
redirect url <url>	Redirect using URL. The URL is an ASCII string of up to 128 characters other than the following characters. {, }, , \, ^, [,], `. Refer to RFC-2396

Default Not set.

Mode Wireless Network Passpoint 802.11u Configuration

Example To set the network authentication type as online-enrollment with a redirect URL, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# network-auth-
type online-enrollment redirect-url example.com
```

To delete the network authentication type online-enrollment, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# no network-
auth-type online-enrollment
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

network-type (wireless-network-passpoint-dot11u)

Overview Use this command to select the access network type.

Use the **no** variant of this command to revert to the default access network type.

Syntax network-type {private|guest-private|chargeable-public| free-public|personal-device|emergency|test|wildcard}
no network-type

Parameter	Description
private	Private network
guest-private	Private network with guest access
chargeable-public	Chargeable public network
free-public	Free public network
personal-device	Personal device network
emergency	Emergency service only network
test	Test or experimental network
wildcard	Wildcard

Default Private.

Mode Wireless Network Passpoint 802.11u Configuration

Example To enter the 802.11u configuration mode and set the network access type to free-public, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# network-type
free-public
```

Related commands **show wireless network**
dot11u (wireless-network-passpoint)
passpoint
network-auth-type (wireless-network-passpoint-dot11u)

Command changes Version 5.5.0-2.3: command added

network (wireless)

Overview Use this command to configure a wireless network.
If the network doesn't exist, then this command creates it.
Use the **no** variant of this command to remove a wireless network.

Syntax network <1-65535>

Parameter	Description
<1-65535>	The network ID number

Default Not set.

Mode Wireless Configuration

Usage notes This commands adds a network configuration and enters the network configuration mode.

Example To configure a wireless network with an ID of 20, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
```

Related commands [show wireless network](#)
[vap \(wireless-ap-prof-radio\)](#)
[description \(wireless-network\)](#)
[vlan \(wireless-network\)](#)
[ssid \(wireless-network\)](#)
[hide-ssid \(wireless-network\)](#)
[band-steering \(wireless-network\)](#)
[security \(wireless-network\)](#)
[vap \(wireless-ap-prof-radio\)](#)

Command changes Version 5.4.7-2.4: command added.

operating-class (wireless-network-passpoint-hs20)

Overview Use this command to set the Operating Class for Hotspot 2.0.
Use the **no** variant of this command to revert to the default value.

Syntax `operating-class <HEX-value>`
`no operating-class`

Parameter	Description
<code><HEX-value></code>	Operating Class Indication value in HEX. Refer to Table E-4 of IEEE Std 802.11-2012 Annex E

Default None

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set an Operating Class Indication value of 51, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# operating-class
51
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

operator (wireless-network-passpoint-hs20)

Overview Use this command to configure the operator friendly name, unique entry number, and language code of a Hotspot 2.0 entry.

Use the **no** variant of this command to remove the configuration details of a Hotspot 2.0 entry.

Syntax `operator <operator-id> lang <language-code> friendly-name
<friendly-name>`
`no operator <operator-id>`

Parameter	Description
<code><operator-id></code>	The unique operator entry number. Select from the range 1-10.
<code><language-code></code>	The language code. You can use only 2 or 3 characters as specified in ISO-639. For example: English is 'eng', Japanese is 'jpn'.
<code><friendly-name></code>	The text field used to identify the Hotspot venue operator. You can use up to 252 octets of special characters (utf-8 encode). For example: "Allied Bld.5th floor".

Default Not set

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To configure the language code and operator friendly name on Operator ID 2, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# operator 2 lang
eng friendly-name Allied-Telesis
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

page-proxy-url

Overview Use this command in Captive Portal mode to set the location of the custom page to display for web authentication. This page will be displayed instead of the wireless access point's built-in authentication or click-through page.

Use the **no** variant of this command to remove the URL pointing to the custom web authentication page.

Syntax `page-proxy-url <URL>`
`no page-proxy-url`

Parameter	Description
<URL>	URL of external web server (hostname or dotted IP notation).

Default No custom page is set by default.

Mode Wireless Network Captive Portal Configuration

Example To enable and set the web authentication proxy page, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# page-proxy-url http://
www.mydomain.com/login_page
```

Related commands **enable (wireless-network-cp)**
mac-auth password
mac-auth username
radius auth group (wireless-network-cp)
redirect-url
session-keep

Command changes Version 5.4.9-1.1: command added

passpoint

Overview Use this command to enter the passpoint configuration mode.
Use the **no** variant of this command to revert to the default setting.

Syntax passpoint
no passpoint

Default Not set.

Mode Wireless Network Configuration

Example To enter passpoint configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)#
```

Related commands **show wireless network**
network (wireless)
enable (wireless-network-passpoint)
hs20 (wireless-network-passpoint)
dot11u (wireless-network-passpoint)

Command changes Version 5.5.0-2.3: command added

power (wireless-ap-radio)

Overview Use this command to set the power level for client devices on a wireless Access Point (AP).

Use the **no** variant of this command to return the power level to its default value.

Syntax power <1-100>

no power

Parameter	Description
<1-100>	The percentage power level value.

Default A power level of 100% is the default.

Mode Wireless AP Radio Configuration

Example To set a power level of 30% for radio 2, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap 100
awplus(config-wireless-ap)# radio 2
awplus(config-wireless-ap-radio)# power 30
```

Related commands [show wireless ap](#)
[radio \(wireless-ap\)](#)

Command changes Version 5.4.7-2.4: command added

pre-authentication enable (wireless-sec-wpa-ent)

Overview Use this command to enable WPA-enterprise pre-authentication for Access Points (APs) that have WPA2 clients.

Use the **no** variant of this command to disable WPA-enterprise pre-authentication.

Syntax pre-authentication enable
no pre-authentication enable

Default Enabled.

Mode Wireless Security WPA-enterprise Configuration

Usage notes Enable this option if the AP has WPA2 clients and you want the AP to share the pre-authentication packets from the clients with other access points. If it is enabled, this can speed up authentication for roaming clients who connect to multiple access points. This option does not apply to WPA clients.

The MWS series of devices do not support pre-authentication, therefore, you should **disable** this command on these devices.

Example To disable pre-authentication on a WPA-enterprise configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# no pre-authentication
enable
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added

proxy-arp enable

Overview Use this command to enable proxy ARP on the wireless network. When Downstream Group-Addressed Forwarding (DGAF) is disabled, AlliedWare Plus enables Proxy ARP on the Access Points.

Use the **no** variant of this command to disable proxy ARP.

Syntax proxy-arp enable
no proxy-arp enable

Default Disabled.

Mode Wireless Network Configuration

Example To enable Proxy ARP, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# proxy-arp enable
```

Related commands [show wireless network](#)
[network \(wireless\)](#)

Command changes Version 5.5.0-2.3: command added

proxy-arp-through enable

Overview Use this command to enable the Proxy Arp pass through feature.

This feature allows ARP packets from unknown addresses to pass through to STAs, when proxy ARP is enabled on the AP, rather than dropping them. This speeds up IP resolution for stations such as IP phones.

Use the **no** variant of this command to disable Proxy Arp pass through.

Syntax proxy-arp-through enable
no proxy-arp-through enable

Default Disabled.

Mode Wireless Network Configuration

Example To enable Proxy ARP pass through, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# proxy-arp-through enable
```

Related commands [show wireless network](#)
[proxy-arp enable](#)

Command changes Version 5.5.5-0.2: command added

qos-map-set (wireless-network-passpoint-dot11u)

Overview Use this command to set the QoS map set for 802.11u.
Use the **no** variant of this command to revert to the default value.

Syntax qos-map-set <qos-map>
no qos-map-set

Parameter	Description
<qos-map>	QoS map configuration. • The QoS map is a comma delimited list of decimal values in the range 0-63 or 255. • The maximum number of elements in the list is 29. (21 DSCP Exception + 8 User Priority). Refer to: IEEE Std 802.11-2012, 8.4.2.97. • Total length of QOSMAP < 190. Format: [<DSCP Exceptions[DSCP,UP]>,<UP 0 range[low,high]>,...<UP 7 range[low,high]>

Default 0

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure two DSCP exceptions (53,2 and 22,6), use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# qos-map-set
53,2,22,6,8,15,0,7,255,16,31,32,39,255,255,40,47,255,255
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

radio (wireless-ap)

Overview Use this command to enter **wireless-ap-radio** configuration mode.

Syntax radio <1-3>

Parameter	Description
<1-3>	The radio interface.

Mode Wireless AP Configuration

Example To enter the AP Radio configuration mode, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap local
awplus(config-wireless-ap)# radio 2
awplus(config-wireless-ap-radio)#
```

Related commands

- ap local**
- show wireless ap**
- show wireless ap neighbors**
- show wireless ap clients**
- description (wireless-ap)**
- power (wireless-ap-radio)**

Command changes Version 5.4.7-2.4: command added

radio (wireless-ap-profile)

Overview Use this command to enter AP profile radio configuration mode. Once in this mode, you can create and modify the radio configuration parameters for an AP profile.

Syntax radio <1-3>

Parameter	Description
<1-3>	The radio interface within the AP profile.

Mode Wireless AP Profile Configuration

Example To enter the AP profile radio configuration mode for radio 1, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)#
```

Related commands

- [show wireless ap-profile](#)
- [enable \(wireless-ap-prof-radio\)](#)
- [mode \(wireless-ap-prof-radio\)](#)
- [bandwidth \(wireless-ap-prof-radio\)](#)
- [management-frame-protection enable \(wireless-sec-wpa-psnl\)](#)
- [max-clients](#)
- [channels \(wireless-ap-prof-radio\)](#)
- [vap \(wireless-ap-prof-radio\)](#)

Command changes Version 5.4.7-2.4: command added.

radius accounting enable

Overview Use this command to configure RADIUS accounting on Captive Portal with external RADIUS.

Use the **no** variant of this command to disable RADIUS accounting on Captive Portal.

Syntax radius accounting enable
no radius accounting enable

Default Disabled.

Mode Wireless Network Captive Portal Configuration

Usage notes The server settings used by Captive Portal RADIUS accounting are those configured by the **radius auth group** command. The port number used is the same one set on the primary server by the command **radius-server host**.

Example To configure RADIUS accounting on Captive Portal for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# radius accounting enable
```

Related commands **radius accounting enable**
radius auth group (wireless-network-cp)

Command changes Version 5.5.0-1.3: command added

radius auth group (wireless-network-cp)

Overview Use this command to set the RADIUS server/s that wireless APs use for Captive Portal (web authentication).
Use the **no** variant of this command to remove the RADIUS server/s used for authentication.

Syntax radius auth group {radius|<groupname>}
no radius auth group {radius|<groupname>}

Parameter	Description
radius	Use a RADIUS server registered with the radius-server host command.
<groupname>	Use a RADIUS server that belongs to the specified server group. Use a server group created with the aaa group server radius command.

Default No RADIUS server set by default.

Mode Wireless Network Captive Portal Configuration

Example To use the RADIUS group 'my_rad' for Captive Portal authentication, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# mode radius
awplus(config-wireless-network-cp)# radius auth group my_rad
```

Related commands **aaa group server**
enable (wireless-network-cp)
mac-auth password
mac-auth username
page-proxy-url
radius-server host
redirect-url
session-keep

Command changes Version 5.4.9-1.1: command added

radius auth group (wireless-sec-wpa-ent)

Overview Use this command to set the RADIUS server group used to authenticate clients in a wireless WPA-enterprise.

Use the **no** variant of this command to set the RADIUS server group to the default.

Syntax radius auth group {radius|<group-name>}
no radius auth group

Parameter	Description
radius	Use all RADIUS servers.
<group-name>	Server group name

Default RADIUS (all RADIUS servers).

Mode Wireless Security WPA-enterprise Configuration

Example To set **radius**, which means all RADIUS servers, to authenticate a wireless WPA-enterprise, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# radius auth group radius
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added

redirect-url

Overview Use this command to enable the redirect-url feature. After successful authentication this feature redirects the web browser to the URL specified in the command. If both **session-keep** and **redirect-url** are enabled, session-keep takes precedence.

Use the **no** variant of this command to disable the redirect-url feature.

Syntax `redirect-url <URL>`
`no redirect-url`

Parameter	Description
<code><URL></code>	URL of page to redirect the user to (hostname or dotted IP notation).

Default Not set by default.

Mode Wireless Network Captive Portal Configuration

Example To enable and set the redirect-url for Captive Portal authentication on network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# redirect-url http://
www.mydomain.com/welcome
```

Related commands **captive-portal**
enable (wireless-network-cp)
mac-auth password
mac-auth username
page-proxy-url
radius auth group (wireless-network-cp)
session-keep

Command changes Version 5.4.9-1.1: command added

roaming-oi (wireless-network-passpoint-dot11u)

Overview Use this command to set the Roaming Consortium List. A Roaming Consortium List contains multiple Organisation Identifiers (OIs) whose security credentials can be used to connect to a network.

Use the **no** variant of this command to revert to the default value.

Syntax `roaming-oi <oi-list>`
`no roaming-oi`

Parameter	Description
<code><oi-list></code>	Roaming Consortium List. - You can have multiple OIs in a list - Each OI is between 3 and 15 octets and is configured as a hexadecimal string. - Separate OIs with a comma. - The maximum number of OIs is 15. - The length of a character in the OI-List must be less than 465 including commas.

Default None

Mode Wireless Network Passpoint 802.11u Configuration

Usage notes The Roaming Consortium Element tell a mobile device which roaming consortiums or service providers are available through an AP.

Example To set a Roaming Consortium List containing two OIs, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# roaming-oi
021122,2233445566
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.1: command added.

rts-threshold

Overview Use this command to set the Request to Send (RTS) threshold on a radio using AP Profile local.

This command is only supported on wireless routers.

Use the **no** variant of this command to reset the RTS threshold to the default value.

Syntax `rts-threshold <0-2347>`
`no rts-threshold`

Parameter	Description
<0-2347>	The RTS threshold for the specified radio using the AP Profile local. This is set in octets.

Default 2347.

Mode Wireless AP Profile Radio Configuration

Usage notes Setting a low RTS value sends packets more frequently. This may consume more bandwidth and reduce throughput.

Example To set an RTS threshold of 1000 on radio1, using AP Profile local, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# rts-threshold 1000
```

To reset RTS threshold to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# no rts-threshold
```

Related commands [ap-profile local](#)
[show wireless ap-profile](#)

Command changes Version 5.5.3-1.1: command added

rule (wireless-mac-filter)

Overview Use this command to permit or deny a rule for the currently selected wireless MAC filter.

Syntax rule [permit|deny]

Parameter	Description
permit	Allow the matched frame.
deny	Deny (drop) the matched frame.

Default Deny.

Mode Wireless MAC Filter Configuration

Example To configure the rule to permit MAC filter1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# mac-filter 1
awplus(config-wireless-mac-flt)# rule permit
```

Related commands [wireless-mac-filter \(wireless-ap-prof\)](#)

Command changes Version 5.5.5-1.1: command added

sc-profile

Overview Use this command to add a Smart Connect profile configuration and enter the Smart Connect profile configuration mode.

Use the **no** variant of this command to remove a Smart Connect profile configuration.

Syntax `sc-profile <1-65535>`
`no sc-profile`

Parameter	Description
<code><1-65535></code>	The Smart Connect profile ID.

Default Not set

Mode Wireless AP Profile Configuration

Example To add Smart Connect profile 1 to AP profile 10, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile 10
awplus(config-wireless-ap-prof)# sc-profile 1
```

Related commands [smart-connect-profile](#)
[show wireless ap-profile](#)
[show wireless network](#)

Command changes Version 5.5.0-0.1: command added

security (wireless)

Overview Use this command to configure a wireless security instance and enter a configuration mode. If the instance doesn't already exist, then this command creates it.

Use the **no** variant of this command to remove a wireless security instance.

Syntax security <1-65535> mode {wep|wpa-personal|wpa-enterprise}
no security <1-65535>

Parameter	Description
<1-65535>	Wireless security instance identification number
mode	Security mode
wep	Security mode WEP. This assigns the configuration identifier to config-wireless-sec-wep mode and enters the mode.
wpa-personal	Security mode WPA-Personal. This assigns the configuration identifier to config-wireless-sec-wpa-psnl mode and enters the mode.
wpa-enterprise	Security mode WPA-Enterprise. This assigns the configuration identifier to config-wireless-sec-wpa-ent mode and enters the mode.

Default Not set.

Mode Wireless Configuration

Usage notes You create a wireless security instance by designating a security instance ID and selecting a security mode. The types of security modes are:

- WEP
- WPA-Personal
- WPA-Enterprise

Example To configure and enter the wireless security mode for WPA-Personal, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 10 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)#
```

Related commands [wireless security \(wireless-network\)](#)
[show wireless security](#)

Command changes Version 5.4.7-2.4: command added

security (wireless-network)

Overview Use this command to designate a security configuration identifier for a wireless security configuration.

Use the **no** variant of this command to remove a security configuration identifier.

Syntax security <1-65535>

no security

Parameter	Description
<1-65535>	The wireless security configuration identifier.

Default Not set.

Mode Wireless Network Configuration

Example To assign a security configuration identifier of 10 to wireless network 2, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 2
awplus(config-wireless-network)# security 10
```

Related commands [network \(wireless\)](#)
[show wireless network](#)

Command changes Version 5.4.7-2.4: command added.

session-keep

Overview Use this command to enable the session-keep feature. After successful authentication this feature redirects the web browser back to the originally requested URL. If both **session-keep** and **redirect-url** are enabled, session-keep takes precedence.

Use the **no** variant of this command to disable the session-keep feature.

Syntax session-keep
no session-keep

Default Not set by default.

Mode Wireless Network Captive Portal Configuration

Example To configure session-keep for Captive Portal authentication on network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# session-keep
```

Related commands **captive-portal**
enable (wireless-network-cp)
mac-auth password
mac-auth username
page-proxy-url
radius auth group (wireless-network-cp)
redirect-url

Command changes Version 5.4.9-1.1: command added

session-key-refresh-action

Overview Use this command to set the action after the interval has expired for the session key used in a WPA-enterprise security configuration.

Use the **no** variant of this command to revert to the default action.

Syntax session-key-refresh-action {reauthentication|disconnection}
no session-key-refresh-action

Parameter	Description
reauthentication	The client will be asked to re-authenticate after the session expires.
disconnection	The client will be disconnected when the session expires.

Default Reauthentication.

Mode Wireless Security WPA-enterprise Configuration

Usage notes This command will not work if the **session-key-refresh-interval** command is set to a non-zero value.

Example For a WPA-enterprise configuration, to set disconnect as the action after the expire session-key refresh interval, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 100 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# session-key-refresh-action
disconnection
```

Related commands [show wireless security](#)
[session-key-refresh-interval](#)

Command changes Version 5.5.1-2.1: command added

session-key-refresh-interval

Overview Use this command to set the refresh interval for the session key used in a WPA-enterprise security configuration.

Use the **no** variant of this command to set the refresh interval to the default.

Syntax session-key-refresh-interval <0-86400>
no session-key-refresh-interval

Parameter	Description
<0-86400>	The refresh interval in seconds.

Default The default refresh interval is 0 seconds.

Mode Wireless Security WPA-enterprise Configuration

Usage notes This command is for TQ series devices only.

Example To set 7200 seconds as the session key refresh rate, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wep-ent)# session-key-refresh-interval 7200
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added

session-timeout-action (wireless network-cp)

Overview Use this command to limit the connection time for clients on a Captive Portal session. When the session times-out, the client will either be presented with the authentication page or be disconnected.

Use the **no** variant of this command to revert to the default action.

Syntax session-timeout-action {reauthentication|disconnection}
no session-timeout-action

Parameter	Description
reauthentication	The client must re-authenticate before continuing to use the Captive Portal session.
disconnection	The client will be disconnected when the Captive Portal session expires. The client can decide whether or not to go through the process of re-authentication.

Default Reauthentication.

Mode Wireless Network Captive Portal Configuration

Usage notes This command will not work if the **session-timeout-interval** command is set to a non-zero value.

Example To disconnect an AP after its Captive Portal session has expired, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# session-timeout-action
disconnection
```

Related commands [show wireless network](#)
[session-timeout-interval \(wireless network-cp\)](#)

Command changes Version 5.5.1-2.1: command added

session-timeout-interval (wireless network-cp)

Overview Use this command to set the session-timeout-interval for authenticated clients in a Captive Portal configuration.

Use the **no** variant of this command to revert to the default session-timeout-interval value.

Syntax session-timeout-interval <0-86400>
no session-timeout-interval

Parameter	Description
<0-86400>	The session-timeout-interval value in seconds. To disable the timeout function, set a value of '0' seconds.

Default 3600 seconds.

Mode Wireless Network Captive Portal Configuration

Example To configure a session-timeout-interval of 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# session-timeout-interval
1800
```

Related commands [show wireless network](#)
[session-timeout-action \(wireless network-cp\)](#)
[session-key-refresh-interval](#)

Command changes Version 5.5.1-2.1: command added

show debugging wireless

Overview Use this command to see what debugging is turned on for wireless management.

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

Syntax show debugging wireless

Mode User Exec and Privileged Exec

Example awplus# show debugging wireless

Output The following shows typical output.

Example output from the show debugging wireless command

```
awplus#show debugging wireless
Wireless debugging is on
Wireless all modules debugging is on
Wireless warning level debugging is on
```

Related commands [show wireless](#)

show wireless

Overview Use this command to show the overall wireless status information.

Syntax show wireless

Mode Privileged Exec

Example To show the overall wireless status on a device, use the command:

```
awplus# show wireless
```

Output

```
awplus#show wireless  
Wireless Controller Mode ..... Local
```

Related commands [ssid \(wireless-network\)](#)

Command changes Version 5.4.7-2.4: command added.

show wireless ap

Overview Use this command to display the configuration and status of wireless Access Points (APs).

Syntax show wireless ap local [brief|status|detail]

Parameter	Description
local	Display the local AP information.
brief	Display the brief configuration details of APs.
status	Display the status of APs.
detail	Display the detailed status and device information of APs.

Mode Privileged Exec

Example To display the status and configuration of wireless APs, use the following command:

```
awplus# show wireless ap local
```

Output The following shows typical output.

Example output from show wireless ap local

```
awplus#show wireless ap local
AP ID Local:
Description .....
AP Profile ..... local
IP Address ..... 127.0.0.1
MAC Address ..... 0000.0000.0000
Serial .....
Firmware Version .....
Management Status ..... Discovering
Configuration Status ..... Not Configured (Modified)
Crash Log Status ..... -
Clients..... 0
Sysup time..... -
Operational Status:
  Reboot Status ..... -
  Firmware Upgrade Status ..... -
  Configuration Apply Status .... -
  Auto Channel Power Status ..... -
```

Output To display a brief (summary), use the following command:

```
awplus# show wireless ap local brief
```

Example output from show wireless ap local brief

```
awplus#show wireless ap local brief
ID      Description Status  Prof  IP Address      MAC Address
-----
Local           Enable  local 127.0.0.1      0000.0000.0000
```

Output To display AP status, use the following command:

```
awplus# show wireless ap status
```

```
awplus# show wireless ap status
ID      FW ver      Manage rupt Config  c Clnt Uptime
-----
Local 0.0.0-0.0  Managd ---- Succeed -    0      66385
```

Related commands

- [description \(wireless-ap\)](#)
- [radio \(wireless-ap-profile\)](#)
- [channels \(wireless-ap-prof-radio\)](#)
- [description \(wireless-ap\)](#)

Command changes Version 5.4.7-2.4: command added.

show wireless ap capability

Overview Use this command to display the configured specifications of a supported wireless Access Point (AP).

Syntax show wireless ap capability
show wireless ap capability hwtype <modelname>
show wireless ap capability hwtype {tq|mws} [single|dual|triple]
[spec {11ac|11ax|11n}] [radio {1|2|3}] [country <country-
code>]

Parameter	Description
hwtype	To specify the display of a hardware type. When omitted, all hardware types will be displayed.
<modelname>	The model name of the wireless AP capabilities to be displayed. For example: • at-tq6702gen2-r for the TQ6702 GEN2-R • at-tq7403-r for the TQ7403-R
tq	Display hardware type AT-TQ series only.
mws	Display hardware type AT-MWS series only.
single	Display information for only APs with a single radio.
dual	Display information for only APs with dual radios.
triple	Display information for only APs with triple radios.
spec	To specify the display of an IEEE wireless networking standard mode. When omitted, all modes are displayed.
11ac	Display information for the 802.11ac mode only.
11ax	Display information for the 802.11ax mode only.
11n	Display information for the 802.11n mode only.
radio	To specify a radio bandwidth. When omitted, all radio bandwidths are displayed.
1	Display information for radio 1 (bandwidth 2.4GHz only).
2	Display information for radio 2 (bandwidth 5GHz only).
3	Display information for radio 3.
country	To specify the display for a country. When omitted, the default country will be displayed.
<country-code>	Display the specified country code. The default country code is 'jp' for Japan or 'us' for other regions.

Mode User Exec and Privileged Exec

Output The following shows typical output.

Example output from show wireless ap capability

```
awplus#show wireless ap capability
Country: nz
```

Hwtype	Radios	Spec	Band	Radio	Mode	Bandwidths
tq	dual	11ac	-	1	bg	20
					*bg-n	20, 40
					n-only-g	20, 40
				2	a	20
					*a-n-ac	20, 40, 80
					n-ac	20, 40, 80
		11ax	-	1	bg	20
					bg-n	20, 40
					*bg-n-ax	20, 40
				2	a	20
					a-n	20, 40
					a-n-ac	20, 40, 80, 8080
		11n	-	1	bg	20
					*bg-n	20, 40
					n-only-g	20, 40
				2	a	20
					*a-n	20, 40
					n-only-a	20, 40
	triple	11ac	-	1	bg	20
					*bg-n	20, 40
				2	a	20
					*a-n-ac	20, 40, 80
				3	a	20
					*a-n-ac	20, 40, 80
		11ax	-	1	bg	20
					bg-n	20, 40
					*bg-n-ax	20, 40
				2	a	20
					a-n	20, 40
					a-n-ac	20, 40, 80
mws	dual	11ac	-	1	*a-n-ac-ax	20, 40, 80
					a	20
					a-n	20, 40
					a-n-ac	20, 40, 80
					*a-n-ac-ax	20, 40, 80
					a	20
				2	bg	20
					*bg-n	20, 40
					n-only-g	20, 40
					a	20
					*n-ac	20, 40, 80
					bg	20
		11n	-	1	*bg-n	20, 40
					n-only-g	20, 40
					a	20
				2	*a-n	20, 40
					n-only-a	20, 40

* means default configuration

Related commands [country-code](#)
[show wireless country-code](#)

Command changes Version 5.4.7-2.4: command added.
Version 5.4.9-1.1: *<modelName>* parameter added.

show wireless ap clients

Overview Use this command to display information about the clients on a wireless Access Point (AP), either:

- this AP (by using the **local** parameter), or
- another AP that this AP is managing through the Wireless Controller (by specifying the other AP's ID).

If no parameters are specified, then all clients on all APs are displayed.

Syntax show wireless ap local clients [radio <1-3>]
show wireless ap [<ap-id-range>|all] clients [radio <1-3>]

Parameter	Description
local	Display wireless clients connected to this AP.
<ap-id-range>	Display information for the selected AP, or a range of APs, from 1 to 65535.
all	Display all APs' clients.
< Radio interface number.	

Mode User Exec and Privileged Exec

Example To display the clients for this AP, use the following command:

```
awplus# show wireless ap local clients
```

To display the clients for all APs, use the following command:

```
awplus# show wireless ap clients
```

Output The following shows typical output.

Example output from show wireless ap clients

awplus#show wireless ap clients							
IP address	MAC address	AP	SSID	RSSI	R Ch	M Age	Tx
192.168.1.100	10f6.0acf.ee87	0	TT-6702G...	-23	1 5	N 00d:00:00:21	154

Related commands [radio \(wireless-ap\)](#)
[wireless disassociate ap local client](#)

Command changes Version 5.4.7-2.4: command added

show wireless ap counter

Overview Use this command to show the transmit and receive statistics of a wireless router.

This command is only supported on Wireless AP Routers.

Syntax show wireless ap local counter

Mode Privileged Exec

Example To display transmit and receive statistics of a wireless router, use the command:

```
awplus# show wireless ap local counter
```

Output The following shows typical output.

Example output from show wireless ap local counter

```
awplus#show wireless ap local counter
AP ID Local:
  Radio ..... 1
  Status ..... Up
  Rx Bytes ..... 0
  Rx Packets ..... 0
  Tx Bytes ..... 1336846
  Tx Packets ..... 16866

  VAP Interface ..... vap1.0
  Status ..... Up
  Rx Bytes ..... 0
  Rx Packets ..... 0
  Tx Bytes ..... 0
  Tx Packets ..... 0
  VAP Interface ..... vap1.1
  Status ..... Up|
  Rx Bytes ..... 0
  Rx Packets ..... 0
  Tx Bytes ..... 0
  Tx Packets ..... 0
  VAP Interface ..... vap1.2
  Status ..... Up
  Rx Bytes ..... 0
  Rx Packets ..... 0
  Tx Bytes ..... 0
  Tx Packets ..... 0
...
```

Related commands [wireless](#)
[show wireless](#)

Command changes Version 5.5.3-1.1: command added

show wireless ap neighbors

Overview Use this command to display the neighboring wireless Access Points (APs) connected to a radio or range of radios. If no parameters are specified, then all configurations are displayed.

Syntax show wireless ap local neighbors [radio <1-3>]

Parameter	Description
	< Radio interface number.
local	Display wireless neighbors connected to the wireless router.

Mode User Exec and Privileged Exec

Example To display wireless AP neighbors, use the following command:

```
awplus# show wireless ap local neighbors
```

Output The following shows typical output.

Example output from show wireless ap local neighbors

```
awplus#show wireless ap local neighbors
-----
BSSID      ESSID                      R Ch  Sig Detected      S
Security Mode
-----
001a.ebab.ced0 meeting-space1      2 124 19  2023-06-27 17:04:43 R
WPA2 PSK (CCMP)
001a.ebab.ced2 meeting-space2      2 124 19  2023-06-27 17:04:43 R
WPA2 PSK (CCMP)
5001.d93a.e654 office              2 116 12  2023-06-27 17:24:14 R
Mixed WPA2/WPA3 Enterprise (CCMP)
```

Related commands [radio \(wireless-ap\)](#)

Command changes Version 5.4.7-2.4: command added.

Version 5.4.8-1.1: display limited to 12500 neighbors

show wireless ap-profile

Overview Use this command to display the AP-profile configuration for a wireless network.

Syntax show wireless ap-profile [local] [brief]

Parameter	Description
brief	Displays a brief summary of AP-profile configurations.
local	Displays a brief summary of the local AP-profile configuration.

Mode User Exec and Privileged Exec

Output The following shows typical output.

Example output from show wireless ap-profile local brief

awplus#show wireless ap-profile local brief				
ID	Description	Radio 1	Radio 2	Radio 3

1		Enable	Enable	Disable

Output The following shows typical output.

Example output from show wireless ap-profile local

```
awplus#show wireless ap-profile local
AP-PROFILE ID local:
Description .....
Country-Code ..... jp
LED ..... Enable
PoE Color ..... Green
Initialization-Button ..... Enable
Rule ..... -
Captive Portal
Virtual IP Address .....
Files .....
Radio 1:
Status ..... Enable
Mode ..... bg-n-ax
Antenna ..... -
Bandwidth ..... 20
Airtime-Fairness ..... Disable
Max-Clients ..... 200
Channel ..... all
Neighbor AP Detection ..... Enable
Legacy Rates ..... all
MU-MIMO ..... Disable
OFDMA ..... Disable
Zero Wait DFS ..... Disable
RTS Threshold ..... 2347
VAP ..... 0
Network ..... 1
WDS mode ..... None

Radio 2:
Status ..... Enable
Mode ..... a-n-ac-ax
Antenna ..... -
Bandwidth ..... 20
Station-Isolation ..... Disable
Airtime-Fairness ..... Disable
Max-Clients ..... 200
Channel ..... all
Neighbor AP Detection ..... Enable
Legacy Rates ..... all
MU-MIMO ..... Disable
OFDMA ..... Disable
Zero Wait DFS ..... Disable
RTS Threshold ..... 2347
VAP ..... 0
Network ..... 17
WDS mode ..... None
```

Related commands [description \(wireless-ap-prof\)](#)
[country-code](#)
[led enable](#)
[initialization-button enable](#)
[radio \(wireless-ap-profile\)](#)

Command changes Version 5.4.7-2.4: command added

show wireless captive-portal network walled-garden

Overview Use this command to display wireless network walled garden entries for Captive Portal.

Syntax show wireless captive-portal {<network-ID>|all} walled-garden

Parameter	Description
<network-ID>	Display output for the specified wireless network ID or range of network IDs, valid network IDs are <1- 65535>.
all	Display all wireless network walled garden entries.

Mode Privileged Exec

Example To display the walled garden entries for Captive Portal on network 5, use the commands:

```
awplus# show wireless captive-portal network 5 walled-garden
```

Output The following shows typical output.

Example output from show wireless captive-portal network 5 walled-garden

```
awplus#show wireless captive-portal network 5 walled-garden
WALLED GARDEN LIST FOR NETWORK ID 5:
Entries ..... 3
Walled Garden
-----
example.com
1.1.1.1
1.1.1.0/24
```

Related commands [captive-portal virtual-ip](#)
[walled-garden entry](#)

Command changes Version 5.5.0-1.3: command added

show wireless country-code

Overview Use this command to display a list of country codes that an Access Point (AP) can use in a wireless configuration.

Syntax show wireless county-code

Mode User Exec and Privileged Exec

Example To display a list of country codes, use the command:
awplus# show wireless country-code

Output The following shows typical output.

Example output from show wireless country-code

```
awplus#show wireless country-code
Code  Country
-----
AD    Andorra
AE    United Arab Emirates
AF    Afghanistan
AG    Antigua and Barbuda
AI    Anguilla
AL    Albania
AM    Armenia
AN    Netherlands Antilles
AO    Angola
AR    Argentina
AS    American Somoa
AT    Austria
AU    Australia
AW    Aruba
AZ    Azerbaijan
.....
```

Related commands [show wireless ap capability](#)
[country-code](#)

Command changes Version 5.4.7-2.4: command added.

show wireless network

Overview Use this command to display a wireless network configuration.

If you use the **brief** parameter, a summary of the configuration will be displayed, otherwise a detailed version is displayed.

Syntax show wireless network [all] [brief]

Parameter	Description
all	Display the configuration for all wireless networks.
brief	Display a brief summary of the wireless network configuration.

Mode User Exec

Example To display the brief wireless network configuration, use the command:

```
awplus# show wireless network brief
```

Output The following shows typical output.

Example output from show wireless network brief

awplus#show wireless network brief							
ID	VLAN	SSID	H	Sec	ID	MAC-Auth	Web-Auth

1	1	allied24	-		1	-	-
17	1	allied5-1	-		17	-	-

Output The following shows typical output.

Example output from show wireless network

```

Network ID 1:
Description .....
Assigned VLAN ID ..... 1
SSID ..... allied24
Hide SSID ..... -
Band-Steering ..... Disable
Association Advertisement ..... Disable
Duplicate AUTH Received ..... Disconnect
DTIM Period ..... 1
Proxy ARP ..... Disable
BSS Transition Management ..... Disable
Security ID ..... -
Security Mode ..... -
MAC-Auth
Authentication Mode ..... radius
RADIUS group .....
Username
Separator ..... hyphen
Character Case ..... lower-case
Password .....
RADIUS Send Service Type ..... Disable
RADIUS DAS IP Address .....
RADIUS group for Web-Auth .....
Wireless MAC filter ID .....
Inactivity Timer ..... 300
Client Isolation Mode ..... Disabled
Unassociated Client List ..... Not acquire
Airtime Fairness Percentage.... 0
Multicast Unicast Conversion .. Disable

Captive-Portal ..... Disable
Authentication Mode ..... click-through
RADIUS group .....
RADIUS Accounting ..... Disable
External Page URL .....
Redirect URL .....
Session keep ..... Disable
Session Timeout Interval ..... 3600
Session Timeout Action . .... Reauthentication
Page proxy URL .....
Walled Garden Entries ..... 0
DNS Proxy for Walled Garden .. Disable
Passpoint ..... Enable
802.11u
Access Network Type ..... private
Internet Access ..... Enable
Additional Step Required .... Disable
ES Reacheable ..... Disable
Venue Group ..... 7
Venue Type ..... 1
Unauth ES accessible ..... Disable
Homogeneous ESSID .....
Roaming Consortium List .....
Venue Name Information .....
Network Auth Type .....
IP Type Availability v4/v6 .. port-private-nat1/no-exist
Domain Name .....
3GPP Info (MCC,MNC) .....
NAI Realm Information .....
ANQP-element .....
GAS Address 3 Behavior ..... 0
GAS Comeback Delay ..... 0
QoS Map Set configuration ..
Hotspot 2.0
DGAF ..... Enable
L2 Traf Inspect and Filter .. Disable

```



```

ANQP Domain ID ..... 0
Deauth Request Timeout ..... 60
Operator Friendly Name .....
Connection Capability .....
WAN Metrics
  WAN Information ..... 01
  Speed Uplink/Downlink ..... 1000/8000
  Load Uplink/Downlink ..... 240/80
  Load Measure Duration ..... 3000
  Operating Class Indication ..
Network ID 17:
  Description .....
  Assigned VLAN ID ..... 1
  SSID ..... allied5-1
  Hide SSID ..... -
  Band-Steering ..... Disable
  Association Advertisement ..... Disable
  Duplicate AUTH Received ..... Disconnect
  DTIM Period ..... 1
  Proxy ARP ..... Disable
  BSS Transition Management ..... Disable
  Security ID ..... -
  Security Mode ..... MAC-Auth
  Authentication Mode ..... radius
  RADIUS group .....
  Username
    Separator ..... hyphen
    Character Case ..... lower-case
  Password .....
  RADIUS Send Service Type ..... Enable
  RADIUS DAS IP Address ..... 192.168.1.1
  RADIUS group for Web-Auth .....
  Wireless MAC filter ID .....
  Inactivity Timer ..... 300
  Client Isolation Mode ..... Disabled
  Unassociated Client List ..... Acquire
  Airtime Fairness Percentage... 3
  Multicast Unicast Conversion .. Enable
  Captive-Portal ..... Disable
  Authentication Mode ..... click-through
  RADIUS group .....
  RADIUS Accounting ..... Disable
  External Page URL .....
  Redirect URL .....
  Session keep ..... Disable
  Session Timeout Interval ..... 3600
  Session Timeout Action . .... Reauthentication
  Page proxy URL .....
  Walled Garden Entries ..... 0
  DNS Proxy for Walled Garden .. Disable-
Passpoint ..... Enable
  802.11u
    Access Network Type ..... public
    Internet Access ..... Enable
    Additional Step Required .... Enable
    ES Reacheable ..... Enable
    Unauth ES Accessible ..... Enable
    Homogeneous ESSID ..... 1234.5678.9abc
    Roaming Consortium List ..... 021122,02233445566
    Network Auth Type
      Auth Type ..... redirect-http-https
      Redirect URL .....
      http://www.example.com/redirect/me/here
    IP Type Availability v4/v6 .. public/no-exist
    Domain Name ..... example.com,google.com
    3GPP Info (MCC,MNC) ..... 244,91;310,261
    NAI Realm Information
      ID 1:
        Realm Name ..... example.com,example.net
        EAP Method ..... EAP-TLS

```

```
ID 2:
  Realm Name ..... example.com;example.net
  EAP Method ..... EAP-TLS,EAP-TTLS/MSCHAPv2
ANQP-element Configuration
  Info ID 1: Payload ..... 0000
  Info ID 20: Payload ..... 00000000
  GAS Address 3 Behavior ..... 0
  GAS Comeback Delay ..... 1000
  QoS Map Set configuration ...
53,2,22,6,8,15,0,7,255,255,16,31,32,39,255,255,40,47,255,255
Hotspot2.0
DGAF ..... Disable
  L2 Traf Inspect and Filter .. Disable
  ANQP Domain ID ..... 0
  Deauth Request Timeout ..... 60
  Operator Friendly Name
ID 1:
  Language Code ..... jpn
  Friendly Name ..... TestJP
ID 2:
  Language Code ..... eng
  Friendly Name ..... TestNZ
Connection Capability
  IP Protocol 1:
    Port ..... 0
    Status ..... open
  IP Protocol 12:
    Port ..... 80
    Status ..... open
WAN Metrics
  WAN Information ..... 01
  Speed Uplink/Downlink ..... 384/2500
  Load Uplink/Downlink ..... 0/0
  Load Measure Duration ..... 10
  Operating Class Indication .. 51
```

Related commands [network \(wireless\)](#)
[show wireless ap](#)
[description \(wireless-network\)](#)

Command changes Version 5.4.7-2.4: command added.

show wireless security

Overview Use this command to display the wireless security configuration.

Syntax show wireless security [<security-id-range>|all] [brief|detail]

Parameter	Description
<security-id-range>	Display the security configuration for a specified ID range. Specify the ID range using the format <1-65535>
all	Display all wireless security configurations.
brief	Display a brief summary of the security configuration.
detail	Display detailed information about the security configuration, including any security keys.

Mode Privileged Exec

Examples To display a brief summary of the wireless security configuration, use the following command:

```
awplus# show wireless security brief
```

To display a longer summary of the wireless security configuration, use the following command:

```
awplus# show wireless security
```

To display a detailed wireless security configuration, use the following command:

```
awplus# show wireless security detail
```

Output The following shows typical output.

Example output from show wireless security brief

```
awplus# show wireless security brief
ID      Mode      Status  Assigned Network  Assigned WDS
-----
1       wep          Enable  11,13,14,25,40..  65535
2       wpa-psnl     Enable  22-24              2
3       wpa-ent      Disable -                -
4       osen         Enable  -
```

Example output from show wireless security

```
awplus# show wireless security
Security ID 1: Enable
Security Mode ..... wpa
Authentication ..... Both
Type ..... ASCII
Length ..... 64
Index ..... 1
...
```

Example output from show wireless security detail

```
awplus# show wireless security detail
Security ID 1:
Security Mode ..... wpa-personal
Key ..... abcdetgh
Versions ..... wpa2
Ciphers ..... ccmp
Session Key Refresh Interval .. 100
Session Key Refresh Action .... Reauthentication
Bcast Key Refresh Interval .... 100
Management Frame Protection ... Enable(capable)
Dynamic-VLAN ..... Enable
Fast Roaming
Fast Transition ..... Disable
Over-the-DS ..... Disable
Mobility Domain ..... a1b2
RMK-R0 Key Lifetime ..... 10000
Reassociation Deadline ..... 1000
AES Key .....
Radio Resource Management .... Disable
Wireless Network Management .. Disable
...
```

Related commands [security \(wireless-network\)](#)

Command changes Version 5.5.3-1.1: Keys moved to output of **detail** parameter.
Version 5.4.7-2.4: command added.

show wireless wireless-mac-filter

Overview Use this command to display the wireless MAC filter configuration for Autonomous Wave Control.

Syntax show wireless wireless-mac-filter [<mac-filter-range>|all]
[brief]

Parameter	Description
<mac-filter-range>	<1-65535>Display the information for a specified ID or range of IDs.
all	Display the information for all MAC filters.
brief	Display a brief summary of the information

Mode Privileged Exec

Output The following shows typical output.

Example output from show wireless-mac-filter

```
awplus#show wireless wireless-mac-filter

WIRELESS MAC FILTER ID 100:
  Description ..... Floor 1
  Rule..... deny
  Entries ..... 3
  Entries ..... 2
    MAC address    Description
    -----
    1234.5678.abcd PC lab 1
    0987.6543.abcd guest
    abcd.9876.5432

WIRELESS MAC FILTER ID 200:
  Description .....
  Entries ..... 0
```

Related commands

- [description \(wireless-mac-flt\)](#)
- [show wireless ap-profile](#)
- [wireless export](#)
- [wireless import](#)
- [wireless-mac-filter \(wireless\)](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)
- [wireless-mac-filter enable](#)

Command changes Version 5.4.8-2.1: command added

single-channel-scan enable

Overview Use this command to allow single channel scanning on the AP profile radio configuration.

Use the **no** variant of this command to disable single channel scanning for APs of a specified AP profile.

Syntax single-channel-scan enable
no single-channel-scan enable

Default Disabled.

Mode Wireless AP Profile Configuration

Example To enable single channel scan for APs of a specified AP profile, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# enable
awplus(config-wireless-ap-prof-radio)# neighbor-ap-detection
enable
awplus(config-wireless-ap-prof-radio)# single-channel-scan
enable
```

To disable single channel scan for APs of a specified AP profile, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# no single-channel-scan
enable
```

Related commands [show wireless ap profile](#)
[single-channel-scan enable](#)
[neighbor-ap-detection enable](#)

Command changes Version 5.5.5-0.1: command added

single-channel-scan duration

Overview Use this command to set the duration for a single channel Radio Frequency Scan (RFScan).
This value is used in AP-Profile configuration
Use the **no** variant of this command to reset the duration of a single channel RFScan to the default value.

Syntax single-channel-scan duration <10-2000>
no single-channel-scan duration

Parameter	Description
<10-2000>	The scan duration in milliseconds.

Default The default scan duration is 50 milliseconds.

Mode Wireless AP Profile Radio Configuration

Example To set the duration of a single RFScan to 120 milliseconds on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# single-channel-scan
duration 120
```

To reset the duration of a single RFScan to the default value on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# no single-channel-scan
duration
```

Related commands [show wireless ap-profile](#)
[single-channel-scan keep-data-time](#)

Command changes Version 5.5.5-0.2: command added

single-channel-scan interval

Overview Use this command to set the interval time for a single channel Radio Frequency Scan (RFScan).

This value is used in AP-Profile configuration

Use the **no** variant of this command to reset the interval time of a single channel RFScan to the default value.

Syntax single-channel-scan interval <30-120>
no single-channel-scan interval

Parameter	Description
<30-120>	The scan interval time in seconds.

Default The default scan duration is 60 seconds.

Mode Wireless AP Profile Radio Configuration

Example To set the interval time of a single RFScan to 120 milliseconds on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# single-channel-scan
interval 80
```

To reset the interval time of a single RFScan to the default value on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# no single-channel-scan
interval
```

Related commands [show wireless ap-profile](#)
[single-channel-scan keep-data-time](#)
[single-channel-scan duration](#)

Command changes Version 5.5.5-0.2: command added

single-channel-scan keep-data-time

Overview Use this command to set the retention time for data obtained from a single channel Radio Frequency Scan (RFScan).

Use the **no** variant of this command to set the retention time to the default.

This value is used in AP-Profile configuration

Syntax single-channel-scan keep-data-time <1800-7200>
no single-channel-scan keep-data-time

Parameter	Description
<1800-7200>	The retention time to keep the RFScan result in seconds.

Default The default time to keep the RFScan result is 3600 seconds.

Mode Wireless AP Profile Radio Configuration

Example To set the time to keep information of a single RFScan result to 4200 seconds on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# single-channel-scan keep-
data-time 4200
```

To reset the time to keep information of a single RFScan result to the default value on Radio 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# no single-channel-scan
keep-data-time
```

Related commands [show wireless ap-profile](#)

Command changes Version 5.5.5-0.2: command added

smart-connect-profile

Overview Use this command to create a Smart Connect profile and enter the Smart Connect profile configuration mode.

Use the **no** variant of this command to delete a Smart Connect profile from the wireless configuration.

Syntax smart-connect-profile <1-65535>
no smart-connect-profile <1-65535>

Parameter	Description
<1-65535>	The Smart Connect profile ID

Default Not set

Mode Wireless Configuration

Example To configure Smart Connect profile 10 and enter the Smart Connect profile configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# smart-connect-profile 10
awplus(config-wireless-sc-prof)#
```

To delete Smart Connect profile 10, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# no smart-connect-profile 10
```

Related commands

- [show wireless ap-profile](#)
- [wireless](#)
- [smart-connect-profile](#)
- [auto-discovery disable](#)
- [show wireless ap-profile](#)
- [description \(wireless-sc-prof\)](#)
- [ssid \(wireless-sc-prof\)](#)
- [key \(wireless-sc-prof\)](#)

Command changes Version 5.5.0-0.1: command added

ssid (wireless-network)

Overview Use this command to configure the SSID (Service Set Identifier) for the wireless network.

Syntax `ssid <value>`

Parameter	Description
<code><value></code>	The unique alphanumeric description or name of the SSID. The maximum character length is 32.

Default

- for network 1, 'allied24' for VAP0 on Radio 1
- for network 17, 'allied5-1' for VAP0 of Radio 2

Mode Wireless Network Configuration

Usage notes A network must be configured with an SSID of one or more alphanumeric characters. The SSID can be modified, but cannot be deleted.

Example To configure a SSID name for a wireless network, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# ssid GUEST_NETWORK_1
```

Related commands

- [network \(wireless\)](#)
- [show wireless network](#)

Command changes Version 5.4.7-2.4: command added.

ssid (wireless-sc-prof)

Overview Use this command to set the SSID used for wireless communication between APs in a Smart Connect network.

Use the **no** variant of this command to remove the SSID from a Smart Connect profile.

Syntax `ssid <ssid-value>`
`no ssid`

Parameter	Description
<code><ssid-value></code>	The SSID for the Smart Connect network. Enter a string up to 32 characters in length.

Default Not set

Mode Wireless Smart Connect Profile Configuration

Example To set the SSID ID of 10 used for wireless communication between APs in Smart Connect network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# smart-connect-profile 20
awplus(config-wireless-sc-prof)# ssid SC-NETWORK-10
```

Related commands [sc-profile](#)
[show wireless ap-profile](#)
[show wireless network](#)

Command changes Version 5.5.0-0.1: command added

station-isolation enable (wireless-ap-prof-radio)

Overview Use this command to enable the **station-isolation** option. This option designates whether to allow communication between wireless clients which are connected to the same Virtual Access Point (VAP).

Use the **no** variant of this command to disable the station-isolation option on a selected VAP.

Syntax station-isolation enable mode vap
no station-isolation enable

Parameter	Description
enable	Enable the station-isolation option.
vap	Set station-isolation mode 'vap' to each radio of the AP Profile. Note: The commands station-isolation enable and station-isolation enable mode vap are the same. In this case, 'station-isolation enable' is shown in the running-config. The parameter ap is shown on the CLI but not supported.

Default Disabled.

Mode Wireless AP Profile Radio Configuration

Example To set station-isolation mode 'vap' to radio of AP Profile local, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# station-isolation enable
mode vap
```

To reset the station-isolation to the default value, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# no station-isolation
enable
```

Related commands **radio (wireless-ap-profile)**
show wireless ap-profile
client-isolation-mode

Command changes Version 5.4.7-2.4: command added.

type (wireless-sec-wep)

Overview Use this command to assign the key-string type for a wireless security WEP configuration.

Use the **no** variant of this command to reset the assigned WEP key-string type to the default.

Syntax type {ascii|hex}
no type

Parameter	Description
ascii	Use ASCII as the type for the WEP key
hex	Use Hex as the type for the WEP key

Default Hex.

Mode Wireless Security WEP Configuration

Example To configure ASCII as the key-string type for WEP for a wireless security WEP configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10 mode wep
awplus(config-wireless-sec-wep)# type ascii
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

unauth-emergency-service-access enable (wireless-network-passpoint-dot11u)

Overview Use this command to configure unauthenticated access to emergency services. This makes emergency services available to any user, with or without a valid authentication credential.

Use the **no** variant of this command to disable unauthenticated access to emergency services.

Syntax unauth-emergency-service-access enable
no unauth-emergency-service-access enable

Default Disabled.

Mode Wireless Network Passpoint 802.11u Configuration

Example To configure unauthenticated access to emergency services, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# dot11u
awplus(config-wireless-network-passpoint-dot11u)# unauth-
emergency-service-access enable
```

Related commands [show wireless network](#)
[dot11u \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

unassociated-client-list acquire

Overview Use this command to allow unauthenticated client information to be acquired. An unauthenticated client is one that has not been authenticated by the RADIUS server when connecting to the VAP.

This information is stored in the STOAT unassociated client list and used to update the network topology map.

Use the **no** variant of this command to disable gathering unauthenticated client information.

Syntax unassociated-client-list acquire
no unassociated-client-list acquire

Default Disabled.

Mode Wireless Network Configuration

Example To acquire the unassociated client list on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# unassociated-client-list
acquire
```

Related commands [show wireless network](#)
[mac-auth radius auth group \(wireless-network\)](#)
[mac-auth mode](#)
[stoat discovery](#)
[stoat destination](#)
[mac-auth radius send service-type](#)

Command changes Version 5.5.4-0.3: command added.

vap (wireless-ap-prof-radio)

Overview Use this command to assign a network configuration ID to a Virtual Access Point (VAP) on a radio.

Use the **no** variant of this command to remove the network configuration for a VAP.

Syntax vap <0-15> network <1-65535> [wds {none|parent|child}]
no vap <0-15>

Parameter	Description
<0-15>	VAP identification number
network	Designate the relevant network configuration identification for the selected VAP.
<1-65535>	Network configuration of the designated VAP
wds	Designate WDS status to the selected VAP. WDS parent or WDS child are accepted only on VAP 0.

Mode Wireless AP Profile Radio Configuration

Example To associate a network (ID1) AP with VAP 0 as WDS parent, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 2
awplus(config-wireless-ap-prof-radio)# vap 0 network 1 wds
parent
```

Related commands [radio \(wireless-ap-profile\)](#)
[network \(wireless\)](#)
[show wireless ap-profile](#)

Command changes Version 5.4.7-2.4: command added.

versions (wireless-sec-wpa-ent)

Overview Use this command to set the WPA version used for a WPA-enterprise wireless security configuration.

Use the **no** variant of this command to reset the designated version to the default.

Syntax versions <version-list>
no versions

Parameter	Description
<version-list>	The version list. You can use either wpa , wpa2 , wpa3 , or any combination of the three in any order.

Default wpa2.

Mode Wireless Security WPA-enterprise Configuration

Usage notes For MWS series devices, a combination of versions and ciphers are supported as follows:

- versions WPA2 and ciphers CCMP
- versions WPA, WPA2, and ciphers TKIP and CCMP

WPA3 is only supported on TS5403 series devices.

Example To configure both WPA and WPA2 as WPA versions on a security configuration for WPA-enterprise, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 210 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# versions wpa wpa2
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

Version 5.4.9-1.1: **wpa3** parameter added.

versions (wireless-sec-wpa-psnl)

Overview Use this command to set the WPA version used for a WPA-personal wireless security configuration.

Use the **no** variant of this command to reset the designated version to the default.

Syntax versions <version-list>
no versions

Parameter	Description
<version-list>	The version list. You can use either wpa , wpa2 , wpa3 , or any combination of the three in any order.

Default wpa2.

Mode Wireless Security WPA-personal Configuration

Usage notes For MWS series devices, a combination of versions and ciphers are supported as follows:

- versions WPA2 and ciphers CCMP
- versions WPA, WPA2, and ciphers TKIP and CCMP

WPA3 is only supported on TS5403 series devices.

Example To configure both WPA and WPA2 as WPA versions on a security configuration for WPA-personal, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 110 mode wpa-personal
awplus(config-wireless-sec-wpa-psnl)# versions wpa wpa2
```

Related commands [security \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.
Version 5.4.9-1.1: **wpa3** parameter added.

vlan (wireless-network)

Overview Use this command to configure the wireless VLAN that clients belong to.
Use the **no** variant of this command to reset the wireless VLAN to the default.

Syntax vlan <1-4094>
no vlan

Parameter	Description
<1-4094>	VLAN ID number.

Default VLAN1.

Mode Wireless Network Configuration

Example To configure a VLAN ID, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# vlan 100
```

To restore VLAN 20 to its default value, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# no vlan
```

Related commands [network \(wireless\)](#)
[show wireless network](#)

Command changes Version 5.4.7-2.4: command added

walled-garden-dns-proxy enable

Overview Use this command to enable DNS proxy for a walled garden.

Use the **no** variant of this command to disable DNS proxy for a walled garden.

A 'walled garden' is often used in public Wi-Fi networks, such as those in airports, hotels, or cafes, to provide users with access to specific resources (such as a login page or certain informational websites) while preventing unrestricted access to the entire Internet.

The DNS proxy server intercepts DNS queries made by users' devices and redirects them to specific IP addresses associated with the allowed websites or services within the walled garden.

Syntax walled-garden-dns-proxy enable
no walled-garden-dns-proxy enable

Default Disabled.

Mode Wireless Network Captive Portal Configuration

Example To enable DNS proxy for a walled garden, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# walled-garden-dns-proxy
enable
```

Related commands [show wireless network](#)
[walled-garden entry](#)

Command changes Version 5.5.3-2.1: command added

walled-garden entry

Overview Use this command to configure a walled garden for Captive Portal.

On the Internet, a walled garden typically controls a user's access to web content and services. The walled garden directs the user's navigation within particular areas to allow access to a selection of websites or prevent access to other websites.

A common example could be a hotel environment where unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

Use the **no** variant of this command to remove a walled garden on a wireless network that's configured with a Captive Portal.

Syntax `walled-garden entry {<ip-addr>|<ip-addr/mask>|<fqdn>}`
`no walled-garden entry {<ip-addr>|<ip-addr/mask>|<fqdn>}`

Parameter	Description
<code><ip-addr></code>	IPv4 address format, e.g. 1.1.1.1
<code><ip-addr/mask></code>	IPv4 address format with subnet mask, e.g. 1.1.1.0/24
<code><fqdn></code>	FDQN format. Sequence of {LETTER/DIGIT/HYPHEN}.{LETTER/DIGIT/HYPHEN}...while each dotted part of the name (aa or bb or cc in this example) MUST NOT end with HYPHEN and the first character MUST be a LETTER or a DIGIT. And each dotted part (aa or bb or cc in this example) must be 63 characters or less, e.g. example.com or www.example.com You can use a wildcard, e.g.*.com, example.*

Default Not set

Mode Wireless Network Captive Portal Configuration

Example To add a new entry to a walled garden list on Captive Portal for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# captive-portal
awplus(config-wireless-network-cp)# walled-garden entry
example.com
```


Related commands [captive-portal virtual-ip](#)
[show wireless network](#)
[show wireless captive-portal network walled-garden](#)
[show wireless network](#)

Command changes Version 5.5.0-1.3: command added

wan-metrics downlink-load (wireless-network-passpoint-hs20)

Overview Use this command to set the wan-metrics downlink-load for Hotspot 2.0.
Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics downlink-load <0-255>
no wan-metrics downlink-load

Parameter	Description
<0-255>	WAN Metrics Down Link Load value Calculation formula: WAN line load factor (%) /100*255 For example: 75% -> 75/100*255=191

Default 80.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set a WAN Metrics Down Link Load of 191, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics
downlink-load 191
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

wan-metrics downlink-speed (wireless-network-passpoint-hs20)

Overview Use this command to set the wan-metrics downlink-speed for Hotspot 2.0.
Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics downlink-speed <1-4294967295>
no wan-metrics downlink-speed

Parameter	Description
<1-4294967295>	WAN Metrics Down Link Speed (kbps)

Default 8000.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set a WAN Metrics Down Link Speed of 191 kbps, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics
downlink-speed 191
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

wan-metrics info (wireless-network-passpoint-hs20)

Overview Use this command to configure the WAN Metrics Link Status information for Hotspot 2.0.

Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics info <HEX-value>
no wan-metrics info

Parameter	Description
<HEX-value>	A one or two digit hexadecimal number.
	Calculation formula: • (At Capacity << 3) (Symmetric Link << 2) (Link Status & 0x3) Bit placement: • Bit[3]: At Capacity • Bit[2]: Symmetric Link • Bit[1:0]: Link Status At Capacity: Set to 1 to notify you that the line capacity on the WAN side has reached the upper limit. Symmetric Link: Set to 1 to notify you that Uplink/Downlink speed are the same value. Link Status: Configure as shown below: • 1 (0b01) : Link up • 2 (0b10) : Link down • 3 (0b11) : Link in test state

Default 01

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set the WAN Metrics Link Status information, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics info
01
```

Related **show wireless network**
commands **hs20 (wireless-network-passpoint)**

Command Version 5.5.0-2.3: command added
changes

wan-metrics load-measure-duration (wireless-network-passpoint-hs20)

Overview Use this command to set the wan-metrics load measure-duration for Hotspot 2.0.

Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics load-measure-duration <0-65535>
no wan-metrics load-measure-duration

Parameter	Description
<0-65535>	WAN Metrics Load Measure Duration value Calculation formula: Measurement interval (seconds)*10 For example: 2 second interval -> 2*10=20

Default 3000.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set a WAN Metrics Load Measure Duration value of 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics
load-measure-duration 20
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

wan-metrics uplink-load (wireless-network-passpoint-hs20)

Overview Use this command to set the wan-metrics uplink-load for Hotspot 2.0.
Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics uplink-load <0-255>
no wan-metrics uplink-load

Parameter	Description
<0-255>	WAN Metrics Up Link Load value Calculation formula: WAN line load factor (%) /100*255 For example: 75% -> 75/100*255=191

Default 240.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set a WAN Metrics Up Link Load of 191, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics
uplink-load 191
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

wan-metrics uplink-speed (wireless-network-passpoint-hs20)

Overview Use this command to set the wan-metrics uplink-speed for Hotspot 2.0.
Use the **no** variant of this command to revert to the default value.

Syntax wan-metrics uplink-speed <1-4294967295>
no wan-metrics uplink-speed

Parameter	Description
<1-4294967295>	WAN Metrics Up Link Speed (kbps)

Default 1000.

Mode Wireless Network Passpoint Hotspot 2.0 Configuration

Example To set a WAN Metrics Up Link Speed of 10000 kbps, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# passpoint
awplus(config-wireless-network-passpoint)# hs20
awplus(config-wireless-network-passpoint-hs20)# wan-metrics
uplink-speed 10000
```

Related commands [show wireless network](#)
[hs20 \(wireless-network-passpoint\)](#)

Command changes Version 5.5.0-2.3: command added

web-auth radius auth group

Overview Use this command to enable Web authentication of clients with a RADIUS group in a wireless network.

Use the **no** variant of this command to disable Web authentication with a RADIUS group.

Syntax web-auth radius auth group {radius|<group-name>}
no web-auth radius auth group

Parameter	Description
radius	Use a RADIUS group, which means all RADIUS servers.
<group-name>	The RADIUS server group.

Default Not set.

Mode Wireless Network.

Usage notes This command enables Web authentication and designates a RADIUS server group to authenticate clients on a wireless network. RADIUS server groups are defined using the **aaa group server** command. RADIUS server groups can consist of multiple server hosts, but this command only uses two servers.

Example To enable Web authentication with a RADIUS server group, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 10
awplus(config-wireless-network)# web-auth radius auth group
radius
```

Related commands [aaa group server](#)
[network \(wireless\)](#)

Command changes Version 5.4.7-2.4: command added.

wireless

Overview Use this command to enter wireless configuration mode.

Use the **no** variant of this command to reset a wireless configuration to the default.

Syntax wireless
no wireless

Mode Global Configuration

Example To enter wireless configuration mode, use the following commands:

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

To reset the wireless configuration on a wireless router to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no wireless
```

Related commands [show wireless ap-profile](#)
[show wireless network](#)

Command changes Version 5.4.7-2.4: command added.

wireless ap-configuration apply ap local

Overview Use this command to instantly apply a wireless configuration to a wireless AP Router. The configuration applied is generated using commands such as **ap local**, **ap-profile local**, and other related wireless commands.

Syntax wireless ap-configuration apply ap local

Mode Privileged Exec

Example To apply a wireless configuration to a device, use the commands:

```
awplus> enable
awplus# wireless ap-configuration apply ap local
```

Related commands

- security (wireless)**
- ap local**
- show wireless ap-profile**
- ap-profile local**
- network (wireless)**

Command changes Version 5.5.3-1.1: command added

wireless ap-configuration pull ap

Overview Use this command to fetch the current running wireless configuration from the CWM Agent and update the device's running configuration.

Syntax `wireless ap-configuration pull ap local [clean-up]`

Parameter	Description
<code>local</code>	Apply the configuration to the local wireless AP.
<code>clean-up</code>	Clean up unused configurations after pulling. This prevents the configuration files from becoming too large. Target configurations include: Network, Security, RADIUS Server Group, and Wireless MAC Filter.

Mode Privileged Exec

Example To pull the configurations from the local AP, use the commands:

```
awplus> enable
```

```
awplus# wireless ap-configuration pull ap local
```

To clean up configurations from the local AP, use the commands:

```
awplus> enable
```

```
awplus# wireless ap-configuration pull ap clean-up
```

Related commands [ap local](#)

Command changes Version 5.5.5-1.1: command added

wireless disassociate ap local client

Overview Use this command to disconnect access point clients attached to a wireless router.

This command is only supported on wireless routers.

Syntax wireless disassociate ap local client [all|<mac-address>]

Parameter	Description
all	Disassociate all access point clients
mac-address	Disassociate an access point by specifying its MAC address in hexadecimal format. HHHH.HHHH.HHHH

Mode Privileged Exec

Examples To disassociate all access point clients, use the commands:

```
awplus> enable
```

```
awplus# wireless disassociate ap local client all
```

To disassociate an access point client by specifying its MAC address, use the commands:

```
awplus> enable
```

```
awplus# wireless disassociate ap local client 1111.2222.3333
```

Related commands [show wireless ap clients](#)
[ap-profile local](#)
[network \(wireless\)](#)

Command changes Version 5.5.3-1.1: command added

wireless export

Overview Use this command to export MAC filter entries to a CSV file. If the specified file does not exist, it will be created. If the file does exist then it will be overwritten with the new data.

Syntax `wireless export wireless-mac-filter <mac-filter-id> <url>`

Parameter	Description
<code><mac-filter-id></code>	<1-65535>The ID of the MAC filter to export.
<code><url></code>	Path and filename of the export file.

Mode Privileged Exec

Example To export MAC filter '20' to a CSV file named 'whitelist.csv', use the following command:

```
awplus# wireless export wireless-mac-filter 20 flash://whitelist.csv
```

Sample export file:

```
"00:1a:eb:12:34:56","client1"  
"00:1a:eb:12:34:57","client2"  
"00:1a:eb:12:34:58","client3"  
"00:1a:eb:12:34:59","client4"  
"00:1a:eb:12:34:5a","client5"
```

Related commands

- [description \(wireless-mac-ft\)](#)
- [show wireless ap-profile](#)
- [show wireless wireless-mac-filter](#)
- [wireless import](#)
- [wireless-mac-filter \(wireless\)](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)
- [wireless-mac-filter enable](#)

Command changes Version 5.4.8-2.1: command added

wireless import

Overview Use this command to import MAC filter entries from a CSV file. The imported entries can either replace or be appended to the existing entries.

Syntax `wireless import <url> wireless-mac-filter <mac-filter-id> {add|replace}`

Parameter	Description
<url>	Path and filename of the import file.
<mac-filter-id>	<1-65535> The ID of the MAC filter to import the entries to.
add	Add the filter entries to the specified MAC filter
replace	Overwrite the existing MAC filter with the imported entries.

Mode Privileged Exec

Example To add MAC filter entries from the file 'whitelist.csv' to MAC filter '20', use the following command:

```
awplus# wireless import flash://whitelist.csv wireless-mac-filter 20 add
```

Sample import file:

```
"00:1a:eb:12:34:56", "client1"  
"00:1a:eb:12:34:57", "client2"  
"00:1a:eb:12:34:58", "client3"  
"00:1a:eb:12:34:59", "client4"  
"00:1a:eb:12:34:5a", "client5"
```

Related commands

- [description \(wireless-mac-ft\)](#)
- [show wireless ap-profile](#)
- [show wireless wireless-mac-filter](#)
- [wireless export](#)
- [wireless-mac-filter \(wireless\)](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)
- [wireless-mac-filter enable](#)

Command changes Version 5.4.8-2.1: command added

wireless-mac-filter (wireless)

Overview Use this command to configure a wireless MAC filter. If the filter does not already exist it will be created when you issue this command.

Use the **no** variant of this command to remove a wireless MAC filter.

Syntax `wireless-mac-filter <mac-filter-id>`
`no wireless-mac-filter <mac-filter-id>`

Parameter	Description
<code><mac-filter-id></code>	The ID of the MAC filter, in the range 1 to 65535.

Default No MAC filters are set by default.

Mode Wireless Configuration

Example To add a MAC filter with ID '20' and enter configuration mode for that filter, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# wireless-mac-filter 20
awplus(config-wireless-mac-flt)#
```

To remove a MAC filter with ID '20', use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# no wireless-mac-filter 20
```

Related commands

- [description \(wireless-mac-flt\)](#)
- [show wireless ap-profile](#)
- [show wireless wireless-mac-filter](#)
- [wireless export](#)
- [wireless import](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)
- [wireless-mac-filter enable](#)

Command changes Version 5.4.8-2.1: command added

wireless-mac-filter-id

Overview Use this command to enable MAC filtering on a specific Wi-Fi network (VAP). If it is on, you can also choose which MAC filter profile (from the AP Profile) to apply to that network.

For example, to restrict access on the internal network to company-issued devices only, you could enable MAC filtering and apply the staff-approved-devices profile, which contains the MAC addresses of authorized laptops and phones.

Use the **no** variant of this command to disable MAC filtering on a specific VAP network.

Syntax wireless-mac-filter-id [<1-65535>|profile]
no wireless-mac-filter-id

Parameter	Description
profile	Enable Wireless MAC filtering using the configured AP Profile (Global) wireless MAC filter.
<1-65535>	The wireless MAC filter ID.

Default Disabled by default.

Mode Wireless Network Configuration

Example To enable wireless MAC filter 10 on APs that use network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# wireless-mac-filter-id 10
```

To enable Global wireless MAC filtering on VAPs that use network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# wireless-mac-filter-id profile
```

To disable wireless MAC filtering on APs that use network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# no wireless-mac-filter-id
```

Related commands [wireless-mac-filter \(wireless-ap-prof\)](#)

Command changes Version 5.5.5-1.1: command added

wireless-mac-filter (wireless-ap-prof)

Overview Use this command to assign a MAC filter to the wireless AP profile. You can configure the filter as a 'whitelist' or a 'blacklist'.

Use the **no** variant of this command to remove a MAC filter from the AP profile.

Syntax wireless-mac-filter {permit|deny} <mac-filter-id>
no wireless-mac-filter

Parameter	Description
permit	Set the MAC filter as a whitelist.
deny	Set the MAC filter as a blacklist.
<mac-filter-id>	The ID of the MAC filter to assign to the AP profile, in the range 1 to 65535.

Default No MAC filter assigned by default.

Mode Wireless AP Profile Configuration

Example To assign the MAC filter '20' as a whitelist, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# wireless-mac-filter permit 20
```

To remove the MAC filter, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# no wireless-mac-filter
```

Related commands **description (wireless-mac-flt)**
show wireless ap-profile
show wireless wireless-mac-filter
wireless export
wireless import
wireless-mac-filter (wireless)
wireless-mac-filter enable

Command changes Version 5.4.8-2.1: command added

wireless-mac-filter enable

Overview Use this command to enable the MAC filter on a Virtual Access Point (VAP). It will enable the MAC filter based on the filter entry set in the AP profile. Use the **no** variant of this command to disable the MAC filter on a VAP.

Syntax wireless-mac-filter enable
no wireless-mac-filter enable

Default Disabled by default.

Mode Wireless Network Configuration

Example To enable wireless MAC filter on APs that use network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# wireless-mac-filter enable
```

To disable wireless MAC filter on APs that use network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# no wireless-mac-filter enable
```

Related commands

- [description \(wireless-mac-ft\)](#)
- [show wireless ap-profile](#)
- [show wireless wireless-mac-filter](#)
- [wireless export](#)
- [wireless import](#)
- [wireless-mac-filter \(wireless\)](#)
- [wireless-mac-filter \(wireless-ap-prof\)](#)

Command changes Version 5.4.8-2.1: command added

Part 2: Interfaces and Layer 2

11

Bridging Commands

- Contents**
- **Introduction** on page 588
 - **ageing-time** on page 589
 - **bridge** on page 590
 - **bridge-group** on page 591
 - **I3-filtering enable** on page 593
 - **mac-learning** on page 594
 - **show bridge** on page 595
 - **show bridge macaddr** on page 597

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**.

ageing-time

Overview This command specifies the time period that a learned MAC address will remain defined within the bridge's MAC address table.

Use the **no** variant of this command to set the ageing out time back to the default.

Syntax ageing-time <10-1000000>
no ageing-time

Parameter	Description
<10-1000000>	The number of seconds that the MAC addresses will remain in the table.

Default 300 seconds (5 minutes)

Mode Interface Configuration

Examples To change the ageing time on br2 to 60 seconds (1 minute), use the following commands:

```
awplus#configure terminal
awplus(config)#interface br2
awplus(config-if)#ageing-time 60
```

To reset the ageing time back to its default, use the following commands:

```
awplus#configure terminal
awplus(config-if)#no ageing-time
```

To reset the ageing time back to its default, you can also use the following commands:

```
awplus#configure terminal
awplus(config-if)#ageing-time 300
```

Output None

Related commands

- [bridge](#)
- [bridge-group](#)
- [show bridge](#)
- [show bridge macaddr](#)

bridge

Overview Use this command to create a software bridge.
Use the **no** variant of this command to remove the specified bridge.

Syntax bridge <bridge-id>
no bridge <bridge-id>

Parameter	Description
<bridge-id>	The bridge ID (from 1 to 300).

Default No configured bridges

Mode Global Configuration

Usage notes The bridge interface name will be prefixed with 'br' followed by the bridge ID.

NOTE: no bridge 2

% failed to remove interface br2, there are still configured sub-interfaces.

Example To create a bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)#bridge 2
```

To remove the bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)##no bridge 2
```

Related commands [ageing-time](#)
[bridge-group](#)
[show bridge](#)
[show bridge macaddr](#)

Command changes Version 5.5.4-0.1: maximum valid ID number changed to 300

bridge-group

Overview Use this command to add an interface to a bridge. Interfaces that have been added to a bridge will lose their L3 properties.

Use the **no** variant of this command to remove an interface from a bridge.

Syntax bridge-group <0-255> [port-protected]
no bridge-group

Parameter	Description
<0-255>	The ID of the bridge that you are adding the interface to.
port-protected	Interfaces added to a bridge can be added in “protected” mode. Interfaces in this mode that are part of the same bridge-group will be unable to bridge to each other, but communication with unprotected interfaces will be unimpeded. Omitting this option from the command will add the interface in unprotected mode.

Default Interfaces do not belong to any bridges.

Mode Interface Configuration

Usage notes Interfaces can only be part of one bridge, so when removing the bridge no parameters are required.

Interfaces that have been added to a bridge will lose their Layer 3 properties. The bridge will act as the Layer 3 interface. The bridge will provide Layer 2 connectivity between interfaces that are a part of the same bridge-group.

You can attach interfaces such as Ethernet and VTI (Tunnel) to your bridge.

Examples To add eth1 to bridge 2 in unprotected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# bridge-group 2
```

To add eth1 to bridge 2 in protected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# bridge-group 2 port-protected
```

To remove eth1 from bridge 2, 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**

l3-filtering enable

Overview Use this command to enable traffic control for bridged traffic on a bridge interface.

Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

Syntax l3-filtering enable
no l3-filtering enable

Default Traffic control is disabled by default for bridged traffic.

Mode Interface mode for a bridge interface

Example To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

Command changes Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

mac-learning

Overview Use this command to enable FDB MAC address learning on a bridge interface. In some circumstances, FDB MAC address learning on a software-based router bridge is not useful, and it is better to flood the traffic within interfaces associated with the bridge instance, to ensure the traffic reaches its destination.

Use the **no** variant of this command to disable or enable FDB MAC address learning on a bridge.

Syntax `mac-learning`
`no mac-learning`

Default Learning is enabled by default.

Mode Interface mode for a bridge interface

Example To turn off learning on bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# no mac-learning
```

To turn learning on bridge 2 back on, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# mac-learning
```

Command changes Version 5.4.7-0.1: command added

show bridge

Overview Use this command to display detailed information about your bridge(s).

Syntax show bridge [<bridge-list>]

Parameter	Description
<bridge-list>	The bridge/s to display the information about. The <bridge-list> can be: • a single bridge(e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Default Displays detailed information about all bridges, if no <bridge-list> is specified.

Mode Privileged Exec

Examples To display information about all bridges, use the following command:

```
awplus#show bridge
```

To display information about bridge 2, use the following command:

```
awplus#show bridge br2
```

To display information about bridge in the range 1 to 3, use the following command:

```
awplus#show bridge br1-3
```

To display information about bridges 1, and from 3 to 5, use the following command:

```
awplus#show bridge br1,br3-5
```

Output The following shows typical output.

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	

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
<i><bridge-list></i>	The bridge interfaces to display the information about. The <i><bridge-list></i> can be: • a single bridge (e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Mode Global Configuration

Example To display the learned MAC entries for bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# show bridge macaddr br2
```

Output The following shows typical output.

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	eth1	ec:cd:6d:20:c0:fb	no	41
br2	eth1	00:c4:6d:20:c0:e6	no	0
br2	eth1	ec:cd:6d:20:c0:bd	yes	0
...				

Related commands

- ageing-time
- bridge
- bridge-group
- show bridge

12

Ethernet Bonding

- Contents**
- **Introduction** on page 599
 - **aggregator-type** on page 600
 - **bond** on page 601
 - **bond-group** on page 602
 - **show bond** on page 603
 - **show bond info** on page 604

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Ethernet bonding.

In the networking industry, link aggregation and Ethernet bonding are terms often used interchangeably as they both refer to the practice of combining multiple physical network links into a single logical link to increase bandwidth, redundancy, and reliability.

Ethernet bonding is used to refer to static or dynamic (LACP) aggregation configured on router Ethernet ports where the router's CPU manages the link aggregation and the packet hashing and forwarding process is handled in software. Ethernet bond interfaces have names like 'bond1' and the name is independent of the aggregation method in use by the bond.

For a description of static and dynamic link aggregation (LACP), and configuration examples, see the [Link Aggregation and Ethernet Bonding Feature Overview and Configuration Guide](#).

aggregator-type

Overview Use this command to configure the aggregation type used by an Ethernet bond.

The default aggregation type is LACP.

Syntax aggregator-type {lacp|static}

Parameter	Description
lacp	Configures the links in the bond to negotiate with their link partners to form a bond using 802.1AX LACP.
static	Use this to configure the links to act as a bond when LACP negotiation is not required or available on the link partner.

Default LACP

Mode Interface Configuration

Example To configure the links in 'bond1' to use LACP negotiation, use the commands:

```
awplus# configure terminal
awplus(config)# interface bond1
awplus(config-if)# aggregator-type lacp
```

To configure the links in 'bond1' to form a bond (without negotiation), use the commands:

```
awplus# configure terminal
awplus(config)# interface bond1
awplus(config-if)# aggregator-type static
```

Related commands [bond](#)
[bond-group](#)
[show bond](#)

Command changes Version 5.5.3-2.1: command added

bond

Overview Use this command to create or delete an Ethernet bond.

The new bond interface name will be 'bond' and the given bond ID, for example 'bond1'.

A bond interface cannot be deleted if it has any configured sub-interfaces.

Use the **no** variant of this command to remove a bond.

Syntax bond <bond-id>
no bond <bond-id>

Parameter	Description
<bond-id>	<1-16> The ID of the new bond being created.

Default No configured bonds

Mode Global Configuration

Usage notes Ethernet bonding is a way to either improve the throughput or add redundancy to Ethernet links by using a set of interfaces that work together to send the traffic and appear as a single interface to higher layers.

Example To configure a new bond with an ID of 1, use the commands:

```
awplus# configure terminal
awplus(config)# bond 1
```

To delete the bond with an ID of 1, use the commands:

```
awplus# configure terminal
awplus(config)# no bond 1
```

Related commands [aggregator-type](#)
[bond-group](#)
[show bond](#)

Command changes Version 5.5.3-2.1: command added

bond-group

Overview Use this command to associate an Ethernet interface to an Ethernet bond. Interfaces that have been added to a bond will only operate as a member of that bond.

Use the **no** variant of this command to delete an Ethernet interface from a bond.

Syntax bond-group <bond-id>
no bond-group

Parameter	Description
<bond-id>	<1-16> The ID of the new bond that the interface is to be associated with.

Default Ethernet interfaces are not part of a bond by default.

Mode Interface Configuration

Example To add eth1 to bond 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config)# bond-group 1
```

To delete eth1 from a bond, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config)# no bond-group
```

Related commands [aggregator-type](#)
[bond](#)
[show bond](#)

Command changes Version 5.5.3-2.1: command added

show bond

Overview Use this command to show the configuration details of Ethernet bonds configured on a device. If no interface names are specified, the command shows the configuration details of all bonds.

Syntax `show bond [<interface-list>]`

Parameter	Description
<code><interface-list></code>	The interface name of a bond, or a list of bonds. For example <code>bond1</code> or <code>bond1,bond2</code> .

Mode Privileged Exec

Example To show the configuration details of all bonds on a device, use the command:

```
awplus# show bond
```

Output The following shows typical output.

Example output from show bond

awplus#show bond		
Bond Name	Mode	Interfaces

bond1	lacp	eth1 eth2

Related commands [aggregator-type](#)
[bond](#)
[bond-group](#)

Command changes Version 5.5.3-2.1: command added

show bond info

Overview Use this command to show the operational information of a device's Ethernet bonds. If no interface names are specified, the command shows operational information for all bonds.

Syntax show bond info [<interface-list>]

Parameter	Description
<interface-list>	The interface name of a bond, or a list of bonds. For example <i>bond1</i> or <i>bond1,bond2</i> .

Mode Privileged Exec

Example To show the operational information of all bonds, use the command:
awplus# show bond info

Output The following shows typical output.

Example output from show bond info

```
awplus#show bond info
Ethernet Bond Interface Information:

bond1
=====
Mode                               : lacp
Transmit Hash Policy               : layer2
MII Status                        : up
System MAC address                : 88:9d:98:4c:e9:80
Actor Key                         : 7
Partner Key                       : 7
Partner Mac Address               : 00:30:ab:f3:42:8f

Slave Interface                   : eth1
MII Status                       : up
Link Partner Mac Address         : 00:30:ab:f3:42:8f

Slave Interface                   : eth2
MII Status                       : up
Link Partner Mac Address         : 00:30:ab:f3:42:8f
```

Related commands [aggregator-type](#)
[bond](#)
[bond-group](#)
[show bond](#)

Command changes Version 5.5.3-2.1: command added

13

802.1Q Encapsulation Commands

- Contents** • [Introduction](#) on page 606
- [encapsulation dot1q](#) on page 607

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure 802.1Q Encapsulation. For more information, see the [Interface Feature Overview and Configuration Guide](#).

encapsulation dot1q

Overview Use this command to enable 802.1Q encapsulation on Ethernet interfaces, L2 tunnel interfaces (e.g. OpenVPN or L2TPv3 Ethernet pseudowire), or the VLAN-aware bridge 0.

Use the **no** variant of this command to disable 802.1Q encapsulation for the VLAN identified by the VLAN ID (VID).

Syntax `encapsulation dot1q <vid>`
`no encapsulation dot1q <vid>`

Parameter	Description
<vid>	Enter a VLAN ID in the range from 1 through 4094. The VLAN ID identifies the VLAN to which the frames belong. It also identifies the index of the subinterface of the Ethernet interface or Layer 2 tunnel interface.

Default 802.1Q encapsulation is disabled by default on all Ethernet interfaces, Layer 2 tunnel interfaces, and bridge interfaces.

Mode Interface Configuration

Usage notes You should enter the Ethernet interface or tunnel interface configuration mode to enable 802.1Q encapsulation and configure the VID first. Then you can use the VID to configure the sub-interface associated with the Ethernet interface or tunnel interface. Sub-interfaces are logical interfaces. The sub interface index must be the same as the VID. For example, if you configure VID 1 for eth1, then the sub-interface for eth1 is eth1.1. If you configure VID 2 for tunnel20, then the sub-interface for tunnel20 is tunnel20.2.

Examples To enable 802.1Q encapsulation on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth1
awplus(config-if)# encapsulation dot1q 1
```

To enable 802.1Q encapsulation on tunnel interface tunnel20, use the commands:

```
awplus# configure terminal
awuplus(config)# interface tunnel20
awplus(config-if)# encapsulation dot1q 2
```

To enable multiple 802.1Q encapsulation on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth1
awplus(config-if)# encapsulation dot1q 1
awplus(config-if)# encapsulation dot1q 2
awplus(config-if)# encapsulation dot1q 3
```

To disable 802.1Q encapsulation on eth1, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth1
awuplus(config-if)# no encapsulation dot1q 1
```

Related commands **interface (to configure)**
show interface

14

PPP Commands

- Contents**
- **Introduction** on page 610
 - **debug ppp** on page 611
 - **encapsulation ppp** on page 614
 - **interface (PPP)** on page 615
 - **ip address negotiated** on page 616
 - **ip tcp adjust-mss** on page 618
 - **ip unnumbered** on page 620
 - **ipv6 tcp adjust-mss** on page 622
 - **keepalive (PPP)** on page 624
 - **mtu (PPP)** on page 626
 - **peer default ip address** on page 628
 - **peer neighbor-route** on page 630
 - **ppp authentication** on page 632
 - **ppp authentication refuse** on page 634
 - **ppp hostname** on page 636
 - **ppp ipcp dns** on page 638
 - **ppp ipcp dns suffix-list** on page 640
 - **ppp ipcp ip-override** on page 642
 - **ppp password** on page 643
 - **ppp service-name (PPPoE)** on page 645
 - **ppp timeout idle** on page 646
 - **ppp username** on page 647
 - **show debugging ppp** on page 648
 - **show interface (PPP)** on page 649
 - **undebg ppp** on page 652

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](#).

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
<ppp-interface- list>	Specify a PPP interface or a range of PPP interfaces in the range ppp<0-255>. 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 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**
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: IP is up on interface ppp0 [local-IP:
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** to enable PPP encapsulation and create PPP interfaces first.

Syntax `interface <PPP-interface-list>`

Parameter	Description
<code><PPP-interface-list></code>	The PPP interfaces or ports to configure. An interface-list can be: • a PPP interface (e.g. ppp0) • a continuous range of PPP interfaces, separated by a hyphen (e.g. ppp0-ppp2) • a comma-separated non-continuous list of PPP interfaces (e.g. ppp0, ppp2) 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><default-ip-addr></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
```

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
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	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

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 or tunnel interface.

The following tunnel types are supported: GRE (excluding multi-point), IPSEC (excluding multi-point), OpenVPN Tunnel, DS-Lite, and IPv6 Tunneling.

Use the **no** variant of this command to remove the borrowed IP address.

Syntax `ip unnumbered <interface-name>`
`no ip unnumbered`

Parameter	Description
<code><interface-name></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 are Ethernet, loopback, and bridge.

Default IP unnumbered is disabled by default.

Mode Interface Configuration

Usage notes An unnumbered point-to-point interface can process IP packets without explicitly assigning an IP address. This is achieved by borrowing the primary IP address from the specified interface.

Examples To borrow an IP address on a tunnel interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 10.28.0.2/24
awplus(config-if)# exit
awplus(config)# interface tunnel1
awplus(config-if)# ip unnumbered eth1
```

To remove the borrowed IP address from the tunnel interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no ip unnumbered
```

To borrow an IP address on unnumbered PPP from vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip address 6.6.6.6/24
awplus(config-if)# exit
awplus(config)# interface ppp0
awplus(config-if)# ip unnumbered vlan2
```

To remove the borrowed IP address on PPP interface, use the following commands:

```
awplus(config)# interface ppp0
awplus(config-if)# no ip unnumbered
```

To borrow an IP address on a tunnel interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip address 10.28.0.1/24
awplus(config-if)# exit
awplus(config)# interface tunnel1
awplus(config-if)# ip unnumbered vlan2
```

Related commands **show ip interface**
show interface tunnel (L2TPv3)
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
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	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.

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. 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. 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><mtu-size></code>	<code><68-1492></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
```

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
```

Output 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 ppp1
Interface ppp1
  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 tunnel1
  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, ppp1
C       4.1.1.2/32 is directly connected, ppp1
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 ppp1
awplus(config-if)#no peer neighbor-route
awplus(config-if)#exit
awplus(config)#exit
awplus#show interface ppp1
Interface ppp1
  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 tunnel1
  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, ppp1
C       192.168.10.0/24 is directly connected, vlan1
```

Related commands [show interface \(PPP\)](#)
[show ip route](#)

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><hostname></code>	Specify this parameter to use an alternate hostname for PPP EAP and CHAP authentication instead of the hostname specified by the hostname 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><primary></code>	Specify the primary DNS address for a given PPP interface to the peer.
<code><secondary></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><domain-list-name></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 [encrypted] <password>
no ppp password

Parameter	Description
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.
<password>	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](#)

Command changes Version 5.5.4-0.1: **encrypted** parameter added

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><service-name></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. 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. 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
<0-99999>	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><username></code>	Specify a login name for the user. 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 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 ppp<0-255>. 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
```

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><ppp_index></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
```

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
```

Example output from the show interface command for a PPP0 interface, stating that the interface is unnumbered

```
awplus#show interface ppp0

Interface ppp0
Link is UP, administrative state is UP
Hardware is PPP
Interface is unnumbered. Using IPv4 address of vlan10 (2.2.2.2)
index 16778240 metric 1 mtu 1492
<UP,POINT-TO-POINT,RUNNING,NOARP,MULTICAST>
PPP is running over interface eth2
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
```

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#show 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
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#
```

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](#)

undebbug 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 undebbug ppp [interface <ppp-interface-list>]

Parameter	Description
<ppp-interface-list>	Specify a PPP interface or a range of PPP interfaces in the range ppp<0 - 255>. 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# undebbug ppp
```

To disable PPP debugging for PPP interfaces ppp0, enter the below command:

```
awplus# undebbug ppp interface ppp0
```

To disable PPP debugging for PPP interfaces ppp0 through ppp2, enter the below command:

```
awplus# undebbug ppp interface ppp0-ppp2
```

To disable PPP debugging for PPP interfaces ppp0 and ppp2, enter the below command:

```
awplus# undebbug ppp interface ppp0,ppp2
```


Related
commands

- debug ppp**
- no debug all**
- show debugging ppp**
- undebug all**

15 PPP over Ethernet (PPPoE) Commands

- Contents**
- **Introduction** on page 655
 - **client (pppoe-relay)** on page 656
 - **max-sessions** on page 657
 - **pppoe-relay** on page 658
 - **server (pppoe-relay)** on page 659
 - **show running-config pppoe-relay** on page 660
 - **timeout (pppoe-relay)** on page 661

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Point to Point Protocol over Ethernet (PPPoE) related features. This includes PPPoE Client and PPPoE Relay.

For more information, see the [PPP Feature Overview and Configuration Guide](#).

client (pppoe-relay)

Overview Use this command to configure a PPPoE relay client interface.

Use the **no** variant of this command to remove a PPPoE relay client interface.

Syntax client <client-interface>
no client <client-interface>

Parameter	Description
<client-interface>	The PPPoE relay client interface. The valid interface type is: eth.

Default None.

Mode PPPoE Relay Configuration

Example To configure eth1 as the client interface on PPPoE relay instance 'Telco1', use the commands:

```
awplus# pppoe-relay Telco1  
awplus(config-pppoe-relay)# client eth1
```

To remove the eth1 client interface configured on PPPoE relay instance 'Telco1', use the commands:

```
awplus# pppoe-relay Telco1  
awplus(config-pppoe-relay)# no client eth1
```

Related commands [server \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[max-sessions](#)
[pppoe-relay](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

max-sessions

Overview Use this command to configure the maximum concurrent sessions for a PPPoE relay instance.

Use the **no** variant of this command to set a PPPoE relay maximum concurrent sessions to the default value.

Syntax max-sessions <1-65534>
no max-sessions

Parameter	Description
<1-65534>	The maximum number of concurrent sessions per PPPoE relay instance.

Default 5000

Mode PPPoE Relay Configuration

Example To set the PPPoE relay maximum concurrent sessions to 50, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# max-sessions 50
```

To set the PPPoE relay maximum concurrent sessions to the default, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# no max-sessions
```

Related commands [client \(pppoe-relay\)](#)
[server \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[pppoe-relay](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

pppoe-relay

Overview Use this command to create a PPPoE relay instance and put the device into PPPoE Relay Configuration mode, in which subsequent commands can be entered.

Use the **no** variant of this command to remove the PPPoE relay instance and all its configuration.

Syntax `pppoe-relay <relay-name>`
`no pppoe-relay <relay-name>`

Parameter	Description
<code><relay-name></code>	Name of the PPPoE relay instance

Default None.

Mode Global Configuration

Usage notes PPPoE relay tracks state information for multiple Layer 2 PPPoE sessions, and allows multiple PPPoE client connections to be relayed between one or more client LANs and a WAN.

This allows the PPPoE client connections to have access to one or more service provider PPPoE Access Concentrators - whilst at the same time allowing Layer 3 IP traffic routing from the internal LAN(s) to the Internet.

Use this command to first create a PPPoE relay instance, then add a client and server interface to the instance.

Example To configure a PPPoE relay instance, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay test
awplus(config-pppoe-relay)#
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [timeout \(pppoe-relay\)](#)
- [max-sessions](#)
- [show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

server (pppoe-relay)

Overview Use this command to configure a PPPoE relay server interface.

Use the **no** variant of this command to remove a PPPoE relay server interface.

Syntax server <server-interface>
no server <server-interface>

Parameter	Description
<server-interface>	The PPPoE relay server interface. The valid interface type is: eth.

Default None.

Mode PPPoE Relay Configuration

Example To configure eth1 as the server interface on PPPoE relay instance 'Telco2', use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco2
awplus(config-pppoe-relay)# server eth1
```

To remove the eth1 server interface configured on PPPoE relay instance 'Telco2', use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco2
awplus(config-pppoe-relay)# no server eth1
```

Related commands [client \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[max-sessions](#)
[pppoe-relay](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

show running-config pppoe-relay

Overview Use this command to display the running configuration for PPPoE relay.

Syntax show running-config pppoe-relay [<relay-name>]

Parameter	Description
<relay-name>	Name of the PPPoE relay instance.

Default None.

Mode Privileged Exec

Example To show all PPPoE relay configurations, use the command:

```
awplus# show running-config pppoe-relay
```

To show the PPPoE relay configuration for Telco1, use the command:

```
awplus# show running-config pppoe-relay Telco1
```

Output The following shows typical output.

Example output from show running-config pppoe-relay

```
awplus#show running-config pppoe-relay
pppoe-relay Telco1
  client eth2
  server vlan4
  max-sessions 50
  timeout 100
!
pppoe-relay Telco2
  client eth1
  server vlan1
!
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [timeout \(pppoe-relay\)](#)
- [max-sessions](#)
- [pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

timeout (pppoe-relay)

Overview Use this command to configure the PPPoE relay idle session timeout.

Use the **no** variant of this command to set the PPPoE relay idle session timeout to the default value.

Syntax timeout {0|<30-86400>}
no timeout

Parameter	Description
0	Sets the idle session timeout to never terminate PPPoE relay sessions.
<30-86400>	The PPPoE relay idle session timeout in seconds.

Default 600 seconds.

Mode PPPoE Relay Configuration

Example To set the PPPoE relay idle session timeout to 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# timeout 1800
```

To set the PPPoE relay idle session timeout to never timeout, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# timeout 0
```

To set the PPPoE relay idle session timeout to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# no timeout
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [max-sessions](#)
- [pppoe-relay](#)
- [show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

Part 3: Routing

16 IP Addressing and Protocol Commands

- Contents**
- **Introduction** on page 665
 - **arp** on page 666
 - **arp log** on page 668
 - **arp opportunistic-nd** on page 672
 - **arp-loose-check** on page 674
 - **arp-reply-bc-dmac** on page 676
 - **clear arp-cache** on page 677
 - **debug ip packet interface** on page 679
 - **ip address (IP Addressing and Protocol)** on page 682
 - **ip directed-broadcast** on page 684
 - **ip forwarding** on page 686
 - **ip forward-protocol udp** on page 687
 - **ip helper-address** on page 689
 - **ip icmp error-interval** on page 691
 - **ip icmp-timestamp** on page 692
 - **ip limited-local-proxy-arp** on page 693
 - **ip local-proxy-arp** on page 694
 - **ip proxy-arp** on page 696
 - **ip redirects** on page 697
 - **ip tcp synack-retries** on page 698
 - **ip tcp timeout established** on page 699
 - **ip tcp-timestamp** on page 700
 - **ip unreachable** on page 701
 - **local-proxy-arp** on page 704
 - **ping** on page 705
 - **show arp** on page 708
 - **show debugging ip packet** on page 711
 - **show ip flooding-nexthops** on page 713
 - **show ip forwarding** on page 714
 - **show ip interface** on page 715
 - **show ip interface vrf** on page 716
 - **show ip sockets** on page 718
 - **show ip traffic** on page 722
 - **tcpdump** on page 724
 - **traceroute** on page 725
 - **undebg ip packet interface** on page 726

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](#).

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.

If VRF-lite is configured, you can add ARP entries to either the global cache or for a specific VRF instance.

The **no** variant of this command removes the static ARP entry. Use the **clear arp-cache** to remove the dynamic ARP entries in the ARP cache.

Syntax `arp <ip-addr> <mac-address> [alias]`
`no arp <ip-addr>`

Syntax (VRF-lite) `arp [vrf <vrf-name>] <ip-addr> <mac-address> [<port-number>]`
`[alias]`
`no arp [vrf <vrf-name>] <ip-addr>`

Parameter	Description
<code><ip-addr></code>	The IPv4 address of the device you are adding as a static ARP entry.
<code><mac-address></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>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.
<code>vrf</code>	Apply this command to a VRF instance.
<code><vrf-name></code>	The name of the VRF instance.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4566 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2533.4566 alias
```

Example (VRF-lite) To apply the above example within a VRF instance called red use the following commands:

```
awplus# configure terminal
awplus(config)# arp vrf red 10.10.10.9 0010.2533.4566 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 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 The following shows typical output.

Output from show log | include ARP_LOG after enabling ARP logging using arp log. Note that this output uses HHHH.HHHH.HHHH format.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG eth1 add
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG eth1 del
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG eth1 add
0030.940e.136b (192.168.2.20)
2022 Mar 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Output from show log | include ARP_LOG after enabling ARP logging using arp log mac-address format ieee. Note that this output uses HH-HH-HH-HH-HH-HH format.

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG eth1 add 00-17-9a-b6-03-
(192.168.2.12)
2022 Mar 6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG eth1 add 00-03-37-6b-a6-
(192.168.2.10)
2022 Mar 6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-30-94-0e-13-
(192.168.2.20)
2022 Mar 6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-17-9a-b6-03-
(192.168.2.12)
2022 Mar 6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-03-37-6b-a6-
(192.168.2.10)
2022 Mar 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

The following table lists the parameters shown in the output of the **show log | include ARP_LOG** command. The ARP log message format is:

*<date> <time> <severity> <hostname> <program-name>
ARP_LOG <port-number> <vid> <operation> <MAC> <IP>*

Parameters in the output from show log | include ARP_LOG

Parameter	Description
ARP_LOG	Indicates that ARP log entry information follows.
<i><operation></i>	Indicates "add" if the ARP log entry displays an ARP addition. Indicates "del" if the ARP log entry displays an ARP deletion.
<i><MAC></i>	Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the arp log or the arp log mac-address-format ieee command.
<i><IP></i>	Indicates the IP address for the ARP log entry.

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

arp opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global ARP cache. This command changes the behavior for unsolicited ARP packet forwarding on the device.



CAUTION: *Opportunistic neighbor discovery can make your device more vulnerable to ARP/ND cache poisoning attacks. We recommend disabling it unless necessary.*

When using VRF-lite, you can use this command to enable opportunistic neighbor discovery for a named VRF instance.

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

Syntax (VRF-lite) arp opportunistic-nd [vrf <vrf-name>]
no arp opportunistic-nd [vrf <vrf-name>]

Parameter	Description
vrf	Apply this command to a VRF instance.
<vrf-name>	The name of the VRF instance.

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.

Note this command enables or disables opportunistic neighbor discovery for a VRF instance if the **vrf** parameter and an instance name are applied. If a VRF instance is not specified, then opportunistic neighbor discovery is enabled or disabled for device ports configured for IPv4.

Examples To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

Example (VRF-lite) To enable opportunistic neighbor discovery for the VRF instance 'blue', enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd vrf blue
```

To disable opportunistic neighbor discovery for the VRF instance 'blue', enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd vrf blue
```

Related commands **ipv6 opportunistic-nd**
show arp
show running-config interface

Command changes Version 5.4.6-2.1: VRF-lite support added.

arp-loose-check

Overview Use this command to let AlliedWare Plus process ARPs that have a sender protocol address from outside the interface's local subnets.

Use the **no** variant of this command to return to the default ARP processing behavior. By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface.

Syntax arp-loose-check
no arp-loose-check

Default Disabled.

Mode Interface Configuration for Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface, to prevent ARP poisoning. This means the packets must have:

- a sender protocol address inside one of the incoming interface's local subnets, and
- a target protocol address equal to one of the incoming interface's IP addresses.

If you enable loose ARP processing and then use the **no** variant of this command to return to default processing, you may need to clear the ARP cache. Use the **clear arp-cache** command. This will remove any undesired existing ARPs.

You cannot use this command at the same time as Proxy ARP. Proxy ARP also allows AlliedWare Plus to process ARPs that have a sender protocol address from outside the interface's local subnets.

Example To process ARPs that have a sender protocol address from outside eth1's local subnets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# arp-loose-check
```

To return to the default behavior on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no arp-loose-check
```

Related commands **arp**
 clear arp-cache
 ip proxy-arp
 show arp

Command changes Version 5.5.2-0.1: command 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 Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Example To allow processing of ARP replies that arrive on eth1 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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.

When running VRF-lite, this command deletes dynamic ARP entries either from the ARP cache of a specific VRF instance, or from the ARP cache of the Global VRF instance. To delete all ARP entries from both the Global VRF instance and all VRF instances, use the command with no parameters. You can optionally specify the IPv4 address for the VRF instance to clear an ARP entry from the ARP cache.

Syntax `clear arp-cache [<ip-address>]`

Syntax (VRF-lite) `clear arp-cache [vrf <vrf-name>|global] [<ip-address>]`

Parameter	Description
<ip-address>	Specifies a specific IPv4 address for a VRF instance whose entries are to be cleared from the ARP cache.
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.
vrf	Apply this command to the specified VRF instance.
<vrf-name>	The VRF instance name.

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
```

Example (VRF-lite) To clear the dynamic ARP entries from the VRF instance named blue, use the commands:

```
awplus# clear arp-cache vrf blue
```

To clear the dynamic ARP entries from the VRF instance named blue with the IPv4 address 192.168.1.1, use the commands:

```
awplus# clear arp-cache vrf blue 192.168.1.1
```

When running VRF-lite, to clear the dynamic ARP entries from the global VRF-lite and all VRF instances, use the command:

```
awplus# clear arp-cache
```

Related commands **arp**
show arp

debug ip packet interface

Overview The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.

If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no** variant of this command disables the **debug ip packet interface** command.

Syntax `debug ip packet interface {<interface-name>|all} [address <ip-address>|verbose|hex|arp|udp|tcp|icmp]`
`no debug ip packet interface [<interface-name>]`

Parameter	Description
<interface-name>	Specify a single Layer 3 interface name (not a range of interfaces) This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface.
all	Specify all Layer 3 interfaces on the device.
<ip-address>	Specify an IPv4 address. If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.
verbose	Specify verbose to output more of the IP packet. If this keyword is specified then more of the packet is shown in the output.
hex	Specify hex to output the IP packet in hexadecimal. If this keyword is specified, then the output for the packet is shown in hex.
arp	Specify arp to output ARP protocol packets. If this keyword is specified, then ARP packets are shown in the output.
udp	Specify udp to output UDP protocol packets. If this keyword is specified then UDP packets are shown in the output.
tcp	Specify tcp to output TCP protocol packets. If this keyword is specified, then TCP packets are shown in the output.
icmp	Specify icmp to output ICMP protocol packets. If this keyword is specified, then ICMP packets are shown in the output.

Mode Privileged Exec and Global Configuration

Examples To turn on ARP packet debugging on eth1, use the command:

```
awplus# debug ip packet interface eth1 arp
```

To turn off IP packet interface debugging on interface eth1, use the command:

```
awplus# no debug ip packet interface eth1
```

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 eth1 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface eth1 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><ip-addr/prefix-length></code>	The IPv4 address and prefix length you are assigning to the interface.
<code>secondary</code>	Secondary IP address.
<code>label</code>	Adds a user-defined description of the secondary IP address.
<code><label></code>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To set the primary IP address on the interface, specify only **ip address** `<ip-addr/prefix-length>`. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

NOTE: Use `show ip address` instead of `show ip address secondary` when you need to view a secondary address configured on an interface. `show ip address` will only show the primary address, not a secondary address for an interface.

Examples To add the IP address 10.10.10.50/24 to the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the 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 an interface, then directed broadcasts received on other interfaces, destined for the subnet on this interface, will be flooded to the subnet broadcast address of this interface.

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 an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes IP directed-broadcast is enabled and disabled per interface. When enabled a directed broadcast packet is forwarded to an enabled interface if received on another subnet.

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is flooded as a broadcast on the destination subnet.

The **ip directed-broadcast** command controls the flooding of directed broadcasts when they reach target subnets. The command affects the final transmission of the directed broadcast on its destination subnet. It does not affect the transit unicast routing of IP directed broadcasts. If directed broadcast is enabled for an interface, incoming directed broadcast IP packets intended for the subnet assigned to the interface will be flooded as broadcasts on that subnet.

If the **no ip directed-broadcast** command is configured for an interface, directed broadcasts destined for the subnet where the interface is attached will be dropped instead of broadcast.

Examples To enable the flooding of broadcast packets via the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip directed-broadcast
```

To disable the flooding of broadcast packets via the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip directed-broadcast
```

Related commands [ip forward-protocol udp](#)
[ip helper-address](#)
[show running-config](#)

Command changes Version 5.5.5-1.1: **access-list** parameter added

ip forwarding

Overview This command enables IP forwarding on your device. When enabled, your device routes IP packets.

The **no** variant of this command disables IP forwarding on your device. Even when IP forwarding is not enabled, the device can still work as an IP host; in particular, it can be managed by IP-based applications, such as SNMP, Telnet and SSH.

Syntax `ip forwarding`
`no ip forwarding`

Default IP forwarding is enabled by default.

Mode Global Configuration

Examples To enable your device to route IP packets, use the commands:

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

To stop your device from routing IP packets, use the commands

```
awplus# configure terminal
awplus(config)# no ip forwarding
```

Related commands [show ip forwarding](#)

ip forward-protocol udp

Overview This command enables you to control which UDP broadcasts will be forwarded to the helper address(es). A UDP broadcast will only be forwarded if the destination UDP port number in the packet matches one of the port numbers specified using this command.

Refer to the IANA site (www.iana.org) for a list of assigned UDP port numbers for protocols to forward using **ip forward-protocol udp**.

Use the **no** variant of this command to remove a port number from the list of destination port numbers that are used as the criterion for deciding if a given UDP broadcast should be forwarded to the IP helper address(es).

Syntax `ip forward-protocol udp <port>`
`no ip forward-protocol udp <port>`

Parameter	Description
<code><port></code>	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** 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 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><ip-addr></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 an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

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 eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip helper-address 192.168.1.100
```

Related commands

- ip forward-protocol udp**
- ip directed-broadcast**
- show running-config**

ip icmp error-interval

Overview Use this command to limit how often IPv4 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds. Use the **no** variant of this command to reset the frequency to the default.

Syntax `ip icmp error-interval <interval>`
`no ip icmp error-interval`

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp error-interval
```

Related commands [ipv6 icmp error-interval](#)

ip icmp-timestamp

Overview Use this command to allow ICMP timestamp request and response packets.

Use the **no** variant of this command to drop ICMP timestamp request and response packets.

You may wish to drop these packets because the ICMP timestamp response contains the device's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, it may be possible to fingerprint devices by analyzing their responses to invalid ICMP timestamp requests.

Syntax `ip icmp-timestamp`
`no ip icmp-timestamp`

Default Allowed

Mode Global Configuration

Example To drop ICMP timestamp packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp-timestamp
```

To allow ICMP timestamp packets again, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp-timestamp
```

Related commands [ip tcp-timestamp](#)

Command changes Version 5.5.2-0.1: command added

ip 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 for Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Usage This command allows you to stop MAC address resolution for specified hosts. Limited local proxy ARP works by intercepting ARP requests for the specified hosts and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of the other hosts through ARP requests.

Limited local proxy ARP ensures that the specified devices cannot send traffic that bypasses Layer 3 routing on your device. This gives you control over which hosts may communicate with one another.

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 subnet. 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 Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable your device to apply Local Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# ip local-proxy-arp
```

To stop your device from doing Local Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
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 Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable your device to do Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# ip proxy-arp
```

To stop your device from doing Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
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
<1-31536000>	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 tcp-timestamp

Overview Use this command to enable TCP timestamp responses.

Use the **no** variant of this command to disable TCP timestamp responses.

You may wish to disable timestamp responses because TCP timestamps may allow other parties to remotely calculate the system uptime and boot time of the device and the device's clock. To prevent this information leaking to potential attackers, we recommend you disable TCP timestamps on the device, unless you need to use them.

Syntax `ip tcp-timestamp`
`no ip tcp-timestamp`

Default Enabled

Mode Global Configuration

Example To disable TCP timestamp responses, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp-timestamp
```

To enable TCP timestamp responses again, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp-timestamp
```

Related commands [ip icmp-timestamp](#)

Command changes Version 5.5.2-0.1: command added

ip unreachable

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 unreachable
no ip 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 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 unreachable** 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.*

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]
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
<i><ip-add/mask></i>	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**

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>]

**Syntax (VRF-
lite)** ping [vrf <vrf-name>] [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.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

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
```

Example (VRF-lite) To ping the IP address 10.10.0.5 from VRF instance 'red', use the following command:

```
awplus# ping vrf red 10.10.0.5
```

NOTE: Unless a cross-domain static or leaked route exists to the destination IP address, you must run this command from within the same routing domain as the address being pinged.

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

Syntax (VRF-lite) show arp [global|vrf <vrf-name>]

Parameter	Description
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.
vrf	Apply this command to the specified VRF instance.
<vrf-name>	The VRF instance name.

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.

With VRF-lite configured, and no additional parameters entered, the command output displays all entries, listed by their VRF instance. By adding either a specific VRF instance or global parameter entry, you can selectively list ARP entries by their membership of a specific VRF instance.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output The following shows typical output.

Example output from the show arp command

awplus#show arp					
IP Address	LL Address	Interface	Port	Type	
10.38.50.2	001a.eb9c.f367	eth1	-	dynamic	
172.31.1.211	001a.eb9c.f367	br1	-	dynamic	
10.38.50.1	000d.b957.6f9d	eth1	-	dynamic	

Example (VRF-lite) To display the dynamic ARP entries in the global routing instance, use the command:

```
awplus# show arp global
```

Output The following shows typical output.

Example output from the show arp global command

awplus#show arp global					
IP Address	LL Address	Interface	Port	Type	
192.168.10.2	0015.77ad.fad8	eth1	-	dynamic	
192.168.1.100	0015.77ad.fa48	eth2	-	static	

Example (VRF-lite) To display the dynamic ARP entries for a VRF instance 'red', use the command:

```
awplus# show arp vrf red
```

Output The following shows typical output.

Example output from the show arp vrf red command

awplus# show arp vrf red					
[VRF: red]					
IP Address	LL Address	Interface	Port	Type	
192.168.10.2	0015.77ad.fad8	eth1	-	dynamic	

Parameters in the output of the show arp command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
LL Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the arp command. Dynamic entries are learned from ARP request/reply message exchanges.
VRF	The name of the VRF instance. The VRF-lite components only display when VRF-lite is configured.

Related commands `arp`
`clear arp-cache`
`ip vrf`

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 The following shows typical output.

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)
...
```

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 The following shows typical output.

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)
...
```

Related [debug ip packet interface](#)
commands [terminal monitor](#)

show ip flooding-nexthops

Overview Use this command to display the static and dynamic ARP entries in the ARP cache that flood packets to multiple ports.

When VRF-lite is configured, you can apply this command to a specific VRF instance.

Syntax `show ip flooding-nexthops`

Syntax (VRF-lite) `show ip flooding-nexthops [vrf <vrf-name>|global]`

Parameter	Description
<code>vrf <vrf-name></code>	VRF instance
<code>global</code>	Global Routing/Forwarding table

Mode User Exec and Privileged Exec

Usage notes To display the flooding nexthop entries associated with a VRF instance, use the **show ip flooding-nexthops vrf** command in User Exec and Privileged Exec mode.

To display the entries in the global ARP table only, use the **show ip flooding-nexthop global** command.

Example To display all of the flooding nexthop entries in the ARP cache, use the command:

```
awplus# show ip flooding-nexthops
```

Output The following shows typical output.

Example output from show ip flooding-nexthops

awplus#show ip flooding-nexthops				
IP Address	MAC Address	Interface	Flooding Mode	Type
11.11.11.10	0300.0000.0011	vlan1	port-group	static
[VRF: test]				
IP Address	MAC Address	Interface	Flooding Mode	Type
10.10.10.10	0100.0000.0000	vlan2	port-group	static

Related commands [show arp](#)

Command changes Version 5.4.8-2.1: command added

show ip forwarding

Overview Use this command to display the IP forwarding status.

Syntax show ip forwarding

Mode User Exec and Privileged Exec

Example awplus# show ip forwarding

Output The following shows typical output.

Example output from the show ip forwarding command

```
awplus#show ip forwarding
IP forwarding is on
```

Related commands [ip forwarding](#)

show ip interface

Overview Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

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

Syntax show ip interface [<interface-list>] [brief]

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show the IP addresses assigned to ppp0, use the command:

```
awplus# show ip interface ppp0 brief
```

Output The following shows typical output.

Example output from the show ip interface brief command

Interface	IP-Address	Status	Protocol
eth0	unassigned	admin up	running
eth0.3	192.168.3.1/24	admin up	running
eth0.2	192.168.2.1/24	admin up	running
lo	unassigned	admin up	running
br0	unassigned	admin up	down

show ip interface vrf

Overview Use this command to display protocol and status information about configured interfaces and their assigned IP addresses in VRF instances.

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

Syntax `show ip interface [vrf <vrf-name>|global]`

Parameter	Description
vrf	A VRF instance.
<vrf-name>	The name of a specific VRF instance.
global	The global routing and forwarding table.

Mode User Exec and Privileged Exec

Examples To display all interfaces and IP addresses associated with a VRF instance 'red', use the command:

```
awplus# show ip interface vrf red
```

Output The following shows typical output.

Example output from show ip interface vrf red

[VRF: red]			
Interface	IP-Address	Status	Protocol
lo1	unassigned	admin up	running
vlan1	192.168.10.1/24	admin up	running

Example To display all interfaces and IP addresses associated with all VRF instances, use the command:

```
awplus# show ip interface
```


Output **Example output from the show ip interface with VRF-lite configured**

Interface	IP-Address	Status	Protocol
eth0	unassigned	admin up	down
lo	unassigned	admin up	running
vlan1	192.168.1.1/24	admin up	running
vlan4	172.30.4.43/24	admin up	down
[VRF: red]			
Interface	IP-Address	Status	
Protocol			
lo1	unassigned	admin up	running
[VRF: blue]			
Interface	IP-Address	Status	
Protocol			
lo2	unassigned	admin up	running

Command changes Version 5.4.6-2.1: VRF-lite support added.

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 The following shows typical output.

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

Parameters in the output from show ip sockets

Parameter	Description
Not showing <number> local connections	This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
Not showing <number> local listening ports	This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
Typ	This column displays the type of the socket. Possible values for this column are: tcp : IP Protocol 6 udp : IP Protocol 17 raw : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.
Local Address	For TCP and UDP listening sockets this shows the destination IP address and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at:www.iana.org/assignments/protocol-numbers
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 .

Parameter	Description
State	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are: LISTEN SYN-SENT SYN-RECEIVED ESTABLISHED FIN-WAIT-1 FIN-WAIT-2 CLOSE-WAIT CLOSING LAST-ACK TIME-WAIT CLOSED RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

show ip traffic

Overview Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

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

Syntax show ip traffic

Mode Privileged Exec

Example To display IP traffic statistics, use the command:

```
awplus# show ip traffic
```

Output The following shows typical output.

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>

Syntax (VRF-lite) tcpdump [vrf <vrf-name>] <line>

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:
awplus# tcpdump ip

Example (VRF-lite) To start a tcpdump on interface vlan2 associated with a VRF instance red, enter the command:
awplus# tcpdump vrf red vlan2

Output

```
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>}`

Syntax (VRF-lite) `traceroute [vrf <vrf-name>] {<ip-addr>|<hostname>}`

Parameter	Description
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

Mode User Exec and Privileged Exec

Example `awplus# traceroute 10.10.0.5`

Example (VRF-lite) `awplus# traceroute vrf red 192.168.0.1`

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**.

17

Domain Name Service (DNS) Commands

- Contents**
- **Introduction** on page 729
 - **accept-invalid-sslcert** on page 730
 - **clear ip dns forwarding cache** on page 731
 - **custom-failure** on page 732
 - **custom-success** on page 733
 - **ddns enable** on page 734
 - **ddns-update-method** on page 735
 - **ddns-update now** on page 737
 - **debug ddns** on page 738
 - **debug ip dns forwarding** on page 739
 - **description (domain-list)** on page 740
 - **domain** on page 741
 - **expect-html-response** on page 742
 - **follow-redirects** on page 743
 - **get-before-submit** on page 744
 - **get-params** on page 745
 - **host-name (ddns-update-method)** on page 746
 - **ip ddns-update-method** on page 747
 - **ip dns forwarding** on page 748
 - **ip dns forwarding cache** on page 750
 - **ip dns forwarding dead-time** on page 752
 - **ip dns forwarding domain-list** on page 753
 - **ip dns forwarding retry** on page 755
 - **ip dns forwarding source-interface** on page 756
 - **ip dns forwarding timeout** on page 757
 - **ip domain-list** on page 758
 - **ip domain-lookup** on page 759
 - **ip domain-name** on page 761
 - **ip name-server** on page 762
 - **ip name-server preferred-order** on page 765
 - **ipv6 ddns-update-method** on page 767
 - **obey-form** on page 768
 - **password (ddns-update-method)** on page 769
 - **ppp ipcp dns** on page 770
 - **ppp ipcp dns suffix-list** on page 772
 - **retry-interval** on page 774
 - **show ddns-update-method status** on page 776

- **show debugging ip dns forwarding** on page 777
- **show hosts** on page 778
- **show ip dns forwarding** on page 780
- **show ip dns forwarding cache** on page 781
- **show ip dns forwarding server** on page 783
- **show ip domain-list** on page 785
- **show ip domain-name** on page 786
- **show ip name-server** on page 787
- **suppress-ipv4-updates** on page 789
- **undebg ddns** on page 790
- **update-interval (ddns-update-method)** on page 791
- **update-url (ddns-update-method)** on page 792
- **use-ipv4-for-ipv6-updates** on page 795
- **username (ddns-update-method)** on page 796

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](#)**.

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

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.

When using VRF-lite, use this command to clear the DNS Relay name resolver cache for either the whole device or for a specific VRF instance.

Syntax clear ip dns forwarding cache

Syntax (VRF-lite) clear ip dns [vrf <name>|global] forwarding cache

Parameter	Description
vrf	Apply this command to the specified VRF instance.
<name>	The name of the specific VRF instance
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.

Mode Privileged Exec

Examples To clear all cached data, use the command:

```
awplus# clear ip dns forwarding cache
```

Example (VRF-lite) To clear the cached data for VRF instance red, use the command:

```
awplus# clear ip dns vrf red forwarding cache
```

To clear the cached data for the default global VRF instance only, use the command:

```
awplus# clear ip dns global forwarding cache
```

Related commands [ip dns forwarding cache](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

custom-failure

Overview Use this command to specify the update server's failure message for Dynamic DNS. You only need to do this if the failure message is different to the ones in DDNS's built-in list.

Use the **no** variant of this command to remove the customized failure message.

Syntax custom-failure <failure-word>
no custom-failure

Parameter	Description
<failure-word>	A word that the update server sends to indicate a failed update.

Default No customized failure message

Mode Dynamic DNS Update Method Configuration

Example If the update server sends a message of 'AllBad' to indicate a failed update, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# custom-failure AllBad
```

Related commands [custom-success](#)
[ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

custom-success

Overview Use this command to specify the update server's success message for Dynamic DNS. You only need to do this if the success message is different to the ones in DDNS's built-in list.

Use the **no** variant of this command to remove the customized success message.

Syntax `custom-success <success-word>`
`no custom-success`

Parameter	Description
<code><success-word></code>	A word that the update server sends to indicate a successful update.

Default No customized success message

Mode Dynamic DNS Update Method Configuration

Example If the update server sends a message of 'AllGood' to indicate a successful update, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# custom-success AllGood
```

Related commands [custom-failure](#)
[ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

ddns enable

Overview Use this command to globally enable or disable DDNS updates. DDNS updates are disabled by default. DDNS configuration will remain when the updates are disabled and DDNS will still be configurable when updates are disabled.

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><method-name></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

- custom-failure**
- custom-success**
- ddns enable**
- ddns-update now**
- debug ddns**
- expect-html-response**
- host-name (ddns-update-method)**
- ip ddns-update-method**
- ipv6 ddns-update-method**
- password (ddns-update-method)**
- retry-interval**
- show ddns-update-method status**
- suppress-ipv4-updates**
- update-interval (ddns-update-method)**
- update-url (ddns-update-method)**
- use-ipv4-for-ipv6-updates**
- username (ddns-update-method)**

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
<method-name>	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><text></code>	Description string, 128 characters maximum. The string may contain spaces.

Mode Domain List

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

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
<domain-string>	• A domain name must only contain a-z, A-Z, 0-9, '-' (en-dash) and '.' (period) characters. • Each sub-section of the domain must not start or end with the '-' character. • Each sub-section must have no more than 64 characters including the '.'. • The last section must not have a '.' at the end. • The whole domain must be less than 254 characters long.

Mode Domain List

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](#)

expect-html-response

Overview Use this command to allow Dynamic DNS to accept HTML formatted responses from the update server (and reject non-HTML responses). You need this if the update server sends HTML responses instead of plain text responses.

Use the **no** variant of this command to stop Dynamic DNS from accepting HTML responses.

Syntax expect-html-response
no expect-html-response

Default Disabled (HTML responses are rejected)

Mode Dynamic DNS Update Method Configuration

Example To configure DDNS to only accept an HTML response, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# expect-html-response
```

Related commands [ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

follow-redirects

Overview Use this command to accept redirects during the initial GET request and during the update. See the command **get-before-submit**. The behavior without this command is to treat redirects as a failure.

Use the **no** variant of this command to disable following redirects.

Syntax follow-redirects
no follow-redirects

Default disabled

Mode Dynamic DNS Update Method Configuration

Example To configure DDNS to accept redirects, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# follow-redirects
```

Related commands **ddns-update-method**
get-before-submit
obey-form

Command changes Version 5.5.1-0.1: command added

get-before-submit

Overview Use this command to make DDNS perform a GET request for the page without any parameters before making the DDNS update submission.
Use the **no** variant of this command to disable this process.

Syntax get-before-submit
no get-before-submit

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes This command may be required if the service you are using either:

- follows a series of redirects before accepting the update submission (see the command **follow-redirects**).
- or
- if the update submission is normally submitted by the browser and contains either a CSRF token or Session ID (see the command **get-params**).

NOTE: Cookies from this GET request are used during the update submission.

Example To configure DDNS to perform a GET request for the page without any parameters before making the DDNS update submission, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
```

Related commands **ddns-update-method**
follow-redirects
get-params
obey-form

Command changes Version 5.5.1-0.1: command added

get-params

Overview Use this command to support update services that use CSRF and other session tracking. This command picks up the required input fields and adds them to the request when it is sent.

Use the **no** variant of this command to remove parameters.

Syntax `get-params <parameter-name>`
`no get-params`

Parameter	Description
<code><parameter-name></code>	A comma separated list of input fields to include the values in the update.

Default No parameters are set

Mode Dynamic DNS Update Method Configuration

Usage notes During the **get-before-submit** stage, the HTML of the page is interpreted, and any input fields that match any of the names in the list are included as extra parameters when the update is submitted.

Example To configure the support update services that use CSRF, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
awplus(config-ddns-update-method)# get-params session,csrf
```

Related commands [ddns-update-method](#)
[get-before-submit](#)

Command changes Version 5.5.1-0.1: command added

host-name (ddns-update-method)

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
<host-name>	The name of the host to be configured in conjunction with the user name and password.

Default None

Mode Dynamic DNS 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-method)# 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-method)# 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><method-name></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.

NOTE:

When running VRF-lite, the DNS Relay functions will apply separately within each VRF instance.

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. Note that when running VRF-lite the number of entries configured will apply to each VRF instance.

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><domain-list-name></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
	ip name-server
	ppp ipcp dns suffix-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

Parameter	Description
<interface-name>	An alphanumeric string that is the interface name.

Default The default is that no interface is set and the device selects the appropriate source IP address automatically.

Mode Global Configuration

Examples To set eth1.2 as the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ip dns forwarding source-interface eth1.2
```

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><domain-name></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.

You can use the **via-relay** parameter to configure the DNS client to use the DNS relay for resolving domain lookups originating from the device. This setup is often preferred because the DNS relay offers additional features not available in the DNS client, such as caching, configurable timeout settings, and more.

You can also use the **via-relay** parameter to enable VRF-aware DNS client lookups.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

Syntax `ip domain-lookup [via-relay]`
`no ip domain-lookup`

Parameter	Description
via-relay	Perform resolution via DNS relay

Mode Global Configuration

Usage notes The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To configure the DNS client to perform resolution via the DNS relay, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup via-relay
awplus(config)# ip dns forwarding
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

Related commands

- ip domain-list**
- ip domain-name**
- ip name-server**
- show hosts**
- show ip name-server**
- ip dns forwarding**

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.

If you are running VRF-lite, you can add IPv4 or IPv6 DNS server addresses for either the global VRF instance or for a specific VRF instance. Host names cannot be resolved from within a VRF instance until you have added at least one name-server to that VRF instance.

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]`

Syntax (VRF-lite) `ip name-server [vrf <name>] <ip-addr>`
`no ip name-server [vrf <name>] <ip-addr>`

Parameter	Description
<code><ip-addr></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>vrf</code>	Apply this command to the specified VRF instance.
<code><name></code>	The name of the specific VRF instance
<code>suffix-list</code>	Specify domain suffixes that should be directed to this name server
<code><domain-list></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
```

Example (VRF-lite) To enable your switch to send DNS queries (on VRF instance RED) to a DNS server with the IPv4 address 10.10.10.5, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server vrf RED 10.10.10.5
```

To enable the VRF-aware DNS client, use the commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup via-relay
awplus(config)# ip dns forwarding
```

Related commands

- ip dns forwarding**
- ip dns forwarding domain-list**
- 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><method-name></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

obey-form

Overview Use this command to read the action URL from the form and submit to that URL instead of the current page's URL. This is needed for forms that don't submit to the current page's URL.

Use the **no** variant of this command to disable form submission.

Syntax obey-form
no obey-form

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes This command applies after the **follow-redirects** and **get-before-submit** commands are applied.

Example To turn on obey-form, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
awplus(config-ddns-update-method)# obey-form
```

Related commands **ddns-update-method**
get-before-submit
follow-redirects

Command changes Version 5.5.0.1: command added

password (ddns-update-method)

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 [encrypted] <password>
no password

Parameter	Description
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.
<password>	The password to be configured in conjunction with the user name and host name.

Default None

Mode Dynamic DNS 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-method)# 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-method)# no password
```

Related commands [ddns-update-method](#)

Command changes Version 5.5.4-0.1: **encrypted** parameter added
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><primary></code>	Specify the primary DNS address for a given PPP interface to the peer.
<code><secondary></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><domain-list-name></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

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><1-3888000></code>	The retry interval in seconds (from 1 second to 4.5 days), after which a failed DDNS update will be retried.
<code><1-100></code>	The maximum number of times a retry is allowed.

Default Disabled

Mode Dynamic DNS 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 The following shows typical output.

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           eth1
IPv4 Address             192.168.10.100
IPv4 Status              Update succeeded
IPv4 Update Result       good 192.168.10.100
IPv6 Interface           eth1
IPv6 Address             333::f195
IPv6 Status              Update succeeded
IPv6 Update Result       good 0333:0000:0000:0000:0000:0000:0000:f195
Last update              Last update Mar 25, 2022 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 The following shows typical output.

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 The following shows typical output.

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
```

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
```

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 **ip domain-list**
commands **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 The following shows typical output.

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

Syntax (VRF-lite) show ip dns [vrf <name>|global] forwarding cache

Parameter	Description
vrf	Apply this command to the specified VRF instance.
<name>	The name of the specific VRF instance
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.

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 The following shows typical output.

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	

Example (VRF-lite) To display the DNS Relay name resolver cache with output for VRF instance RED, use the command:

```
awplus# show ip dns vrf RED forwarding cache
```

Output The following shows typical output.

Example output from the show ip dns forwarding cache command that includes output for VRF instance RED.

```
awplus#show ip dns vrf RED 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

[VRF: RED]
www.example2.com           10.25.1.1.            180
mail.example2.com          www.example2.com        180 CNAME
www.example2.com           10.25.1.1.            180 REVERSE
mail.example2.com          10.25.1.6.            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.

If you are running VRF, you can also use this command to display the status for DNS forwarding name servers operating on a specific VRF instance.

Syntax show ip dns forwarding server

Syntax (VRF-lite) show ip dns [vrf <vrf-name>|global] forwarding server

Parameter	Description
vrf	Apply this command to the specified VRF instance.
<vrf-name>	The name of the specific VRF instance.
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.
forwarding server	Display information about the DNS forwarding name servers for either the device (when not using VRF-lite) or for a specific VRF instance (when using VRF-lite).

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 The following shows typical output.

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

Example (VRF-lite) To display the status of DNS Relay name-servers for VRF-lite instance red, use the command:

```
awplus# show ip dns vrf red forwarding server
```

Output The following shows typical output.

Example output from the show ip dns vrf red forwarding server command

```
awplus#show ip dns vrf red forwarding server

[VRF: red]
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 The following shows typical output.

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 The following shows typical output.

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.

When running VRF-lite, this command displays a list of IPv4 and IPv6 addresses of DNS servers that your device will send DNS requests to for either the global VRF instance or a selected VRF instance.

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

Syntax (VRF-lite) show ip name-server [vrf <name>|global]

Parameter	Description
vrf	A VRF instance
<name>	The name of the specific VRF instance
global	The global VRF instance

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 The following shows typical output.

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
```

Output (VRF-lite) **Example output from the show ip name-server command for the VRF instance "red"**

```
awplus# show ip name-server vrf red

[VRF: red]
 10.10.0.123
 10.10.0.124
2001:0db8:010d::1
```

Related commands [ip domain-lookup](#)
[ip name-server](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

suppress-ipv4-updates

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 Dynamic DNS 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](#)

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-update-method)

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
<1-64800>	Update interval time in minutes (from 1 minute to 45 days).

Default Disabled

Mode Dynamic DNS 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-update-method)

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
<url-name>	The update URL is provided by the DDNS provider and can be configured with the following placeholder tokens: • <USERNAME> • <PASSWORD> • <HOST-NAME> • <IPADDRESS> To specify the values for <USERNAME>, <PASSWORD> and <HOST-NAME>, use the commands username, password and hostname. The value for <IPADDRESS> is populated automatically from the interface IP settings.

Default None

Mode Dynamic DNS 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

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 Dynamic DNS 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](#)

Command changes Version 5.4.7-0.1: command added

username (ddns-update-method)

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
<user-name>	The name of the user to be configured in conjunction with the password and host name.

Default None

Mode Dynamic DNS 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-method)# 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-method)# no username
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

18

IPv6 Commands

- Contents**
- **Introduction** on page 798
 - **clear ipv6 neighbors** on page 799
 - **ipv6 address** on page 800
 - **ipv6 address autoconfig** on page 802
 - **ipv6 address suffix** on page 804
 - **ipv6 enable** on page 805
 - **ipv6 eui64-linklocal** on page 807
 - **ipv6 forwarding** on page 808
 - **ipv6 icmp error-interval** on page 809
 - **ipv6 nd accept-ra-default-routes** on page 810
 - **ipv6 nd accept-ra-pinfo** on page 811
 - **ipv6 nd current-hoplimit** on page 812
 - **ipv6 nd dns search-list** on page 814
 - **ipv6 nd dns-server** on page 815
 - **ipv6 nd managed-config-flag** on page 817
 - **ipv6 nd minimum-ra-interval** on page 819
 - **ipv6 nd other-config-flag** on page 821
 - **ipv6 nd prefix** on page 822
 - **ipv6 nd proxy interface** on page 825
 - **ipv6 nd ra-interval** on page 826
 - **ipv6 nd ra-lifetime** on page 827
 - **ipv6 nd reachable-time** on page 829
 - **ipv6 nd retransmission-time** on page 831
 - **ipv6 nd route-information** on page 833
 - **ipv6 nd router-preference** on page 835
 - **ipv6 nd suppress-ra** on page 836
 - **ipv6 opportunistic-nd** on page 837
 - **ipv6 route** on page 838
 - **ipv6 route vrf** on page 840
 - **ipv6 unreachable** on page 843
 - **ping ipv6** on page 845
 - **show ipv6 forwarding** on page 848
 - **show ipv6 interface** on page 849
 - **show ipv6 neighbors** on page 851
 - **show ipv6 route** on page 852
 - **show ipv6 route summary** on page 855
 - **traceroute ipv6** on page 856

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](#).

clear ipv6 neighbors

Overview Use this command to clear all dynamic IPv6 neighbor entries.

Syntax `clear ipv6 neighbors`

Mode Privileged Exec

Example `awplus# clear ipv6 neighbors`

Related commands [show ipv6 neighbors](#)

ipv6 address

Overview Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax `ipv6 address <ipv6-addr/prefix-length>`
`no ipv6 address <ipv6-addr/prefix-length>`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the **ipv6 enable** command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Examples To assign the IPv6 address 2001:0db8::a2/64 to eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the tunnel tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface ppp0, use the 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**
- 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 an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command to enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface, and enable IPv6.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface.

If SLAAC is not suitable then a network can use stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6) Relay, or hosts can be configured statically. See [ip dhcp-relay server-address](#) for the DHCPv6 Relay server command description and examples. See the [IP Feature Overview and Configuration Guide](#) for more information about DNS Relay.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the [ipv6 enable](#) command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the [ipv6 enable](#) command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 address autoconfig
```

Related commands

- ipv6 address**
- ipv6 enable**
- show ipv6 interface**
- show running-config**

ipv6 address suffix

Overview Use this command to configure the suffix to use when generating an address from prefix information. Any addresses that were created with the EUI-64 suffix will be removed, and new addresses will be added after the next Router Advertisement.

Use the **no** variant of this command to set it back to the default of disabled or set to :: for the same result as the **no** variant.

Syntax `ipv6 address suffix <ipv6-addr-suffix>`
`no ipv6 address suffix`

Parameter	Description
<code><ipv6-addr-suffix></code>	In the format of ::X:X:X:X, for example ::a2d8:0fd8

Default Disabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

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 an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes The **ipv6 enable** command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Default All interfaces default to IPv6-down with no address.

Examples To enable IPv6 with only a link-local IPv6 address on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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**
- show ipv6 route**
- show running-config**

ipv6 eui64-linklocal

Overview When IPv6 is enabled on an interface, an EUI link-local address is generated and installed on the interface. In other words, **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Use the **no** variant of this command to disallow the automatic generation of the EUI-64 link-local address on an IPv6 enabled interface.

Syntax `ipv6 eui64-linklocal`
`no ipv6 eui64-linklocal`

Default The command **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

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 icmp error-interval

Overview Use this command to limit how often IPv6 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds. Use the **no** variant of this command to reset the frequency to the default

Syntax `ipv6 icmp error-interval <interval>`
`no ipv6 icmp error-interval`

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 icmp error-interval
```

Related commands [ip icmp error-interval](#)

ipv6 nd accept-ra-default-routes

Overview Use this command to allow accepting and installing of default routes based on a received RA (Router Advertisement). The default route's destination is set to the source address of the received RA.

Use the **no** variant of this command to disable accepting RA-based default routes.

Syntax `ipv6 nd accept-ra-default-routes`
`no ipv6 nd accept-ra-default-routes`

Default RA-based default routes are accepted by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To enable RA-based default routes on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd accept-ra-default-routes
```

Related commands [ipv6 address](#)
[ipv6 address autoconfig](#)
[ipv6 enable](#)

ipv6 nd accept-ra-pinfo

Overview Use this command to allow the processing of the prefix information included in a received RA (Router Advertisement) on an IPv6 enabled interface.

Use the **no** variant of this command to disable an IPv6 interface from using the prefix information within a received RA.

Syntax `ipv6 nd accept-ra-pinfo`
`no ipv6 nd accept-ra-pinfo`

Default The command **ipv6 nd accept-ra-pinfo** is enabled by default on any IPv6 interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes By default, when IPv6 is enabled on an interface, SLAAC is also enabled. SLAAC addressing along with the EUI-64 process, uses the prefix information included in a received RA to generate an automatic link-local address on the IPv6 interface.

Note: an AlliedWare Plus device will, by default, add a prefix for the connected interface IPv6 address(es) to the RA it transmits. However, this behavior can be changed by using the command **no ipv6 nd prefix auto-advertise**, so there is no guarantee that an RA will contain a prefix.

Example To enable IPv6 on 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 the default of 0, which means no advertised current hop limit is specified.

Syntax `ipv6 nd current-hoplimit <hoplimit>`
`no ipv6 nd current-hoplimit`

Parameter	Description
<hoplimit>	Specifies the advertised current hop limit value. Valid values are from 0 to 255 hops.

Default 0 (No advertised current hop limit specified)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the advertised current hop limit to 2 between IPv6 Routers on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 [ipv6 nd managed-config-flag](#)
commands [ipv6 nd prefix](#)
[ipv6 nd suppress-ra](#)

ipv6 nd dns search-list

Overview Use this command to specify a DNS Search List (DNSSL) to be included in the Router Advertisement for a given IPv6 interface.

Use the **no** variant of this command to remove a specified domain name. If no domain name is specified, then all domain names previously added will be deleted.

Syntax `ipv6 nd dns search-list <domain-name>`
`no ipv6 nd dns search-list [<domain-name>]`

Parameter	Description
<code><domain-name></code>	A string specifying the domain name to be added to the search list. For example, myexample.com

Default No domain search list is included in router advertisements from any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To add the domain name 'myexample.com' to the search list for eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd dns search-list myexample.com
```

To delete all domain names added previously, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd dns search-list
```

Related commands [ipv6 nd suppress-ra](#)

Command changes Version 5.5.0-2.5: command added

ipv6 nd dns-server

Overview Use this command to advertise (in Router Advertisement messages) a DNS server for downstream devices to use.

You can specify either a static IPv6 address or the lowest address from an interface.

Use the **no** variant of this command to delete one or all DNS server addresses.

Syntax `ipv6 nd dns-server {<int>|<ip-add>}`
`no ipv6 nd dns-server [<int>|<ip-add>]`

Parameter	Description
<int>	Advertise the lowest IPv6 address on the selected interface as a DNS server for downstream devices.
<ip-add>	Advertise a particular IPv6 address as a DNS server for downstream devices.

Default No DNS servers are advertised.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To configure eth1 to send RAs and advertise itself as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd suppress-ra
awplus(config-if)# no ipv6 nd accept-ra-pinfo
awplus(config-if)# ipv6 address 2001:DB8::1/64
awplus(config-if)# ipv6 nd dns-server eth1
```

To configure eth1 to send RAs and advertise 2001:DB8::2 as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd suppress-ra
awplus(config-if)# no ipv6 nd accept-ra-pinfo
awplus(config-if)# ipv6 address 2001:DB8::1/64
awplus(config-if)# ipv6 nd dns-server 2001:DB8::2
```

To stop advertising any DNS servers on the selected interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd dns-server
```

Related commands [ipv6 nd accept-ra-pinfo](#)
[ipv6 nd suppress-ra](#)
[show ipv6 interface](#)

ipv6 nd managed-config-flag

Overview Use this command to set the managed address configuration flag, contained within the router advertisement field.

Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.

An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.

Use the **no** variant of this command to reset this command to its default of having the flag unset.

Syntax `ipv6 nd managed-config-flag`
`no ipv6 nd managed-config-flag`

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the **ipv6 nd suppress-ra**. This step is included in the example below.

Example To set the managed address configuration flag on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 **ipv6 nd suppress-ra**
commands **ipv6 nd prefix**
ipv6 nd other-config-flag

ipv6 nd minimum-ra-interval

Overview Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for an interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for an interface.

Syntax `ipv6 nd minimum-ra-interval <seconds>`
`no ipv6 nd minimum-ra-interval`

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.

Default The RA interval for an interface is unset by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the minimum RA interval for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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** implies that the **ipv6 nd other-config-flag** will also be set.

Use **no** variant of this command to reset the value to the default.

Syntax `ipv6 nd other-config-flag`
`no ipv6 nd other-config-flag`

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the **ipv6 nd suppress-ra**. This step is included in the example below.

Example To set the IPv6 other-config-flag on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration.

Use the **no** parameter with this command to reset the IPv6 prefix for an interface in Interface Configuration mode.

Syntax `ipv6 nd prefix <ipv6-prefix/length>`
`ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>`
`ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime> <preferred-lifetime> [no-autoconfig]`
`ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime> <preferred-lifetime> off-link [no-autoconfig]`
`no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]`

Parameter	Description
<code><ipv6-prefix/length></code>	The prefix to be advertised by the router advertisement message. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. The default is X:X::/64.
<code><valid-lifetime></code>	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.
<code><preferred-lifetime></code>	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.
<code>off-link</code>	Specify the IPv6 prefix off-link flag. The default is flag set.
<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. The default is flag set.
<code>all</code>	Specify all IPv6 prefixes associated with the interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Examples To configure the device to issue router advertisements on eth1, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the device to issue router advertisements on eth1, 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 eth1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

To configure the device to issue router advertisements on eth1 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 eth1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
no-autoconfig
```

To reset router advertisements on eth1, so the address prefix of 2001:0db8::/64 is not advertised from the device, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

To reset all router advertisements on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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
<code><interface-name></code>	The name of the Ethernet or Bridge interface to proxy NS and NA from/to. For example eth1 or br1.

Default No ND proxy is enabled

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable neighbor discovery proxy on eth1, and forward NS and NA to eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd proxy interface eth2
```

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
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.

Default 600 seconds.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the **ipv6 nd suppress-ra**. This step is included in the example below.

Example To set the advertisements interval on eth1 to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisements interval on eth1 to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd ra-interval
```

Related commands **ipv6 nd minimum-ra-interval**
ipv6 nd suppress-ra
ipv6 nd prefix

ipv6 nd ra-lifetime

Overview Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

Syntax `ipv6 nd ra-lifetime <seconds>`
`no ipv6 nd ra-lifetime`

Parameter	Description
<seconds>	Time period in seconds. Valid values are from 0 to 9000. Note that you should set this time period to a value greater than the value you have set using the ipv6 nd ra-interval command.

Default 1800 seconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no** version of the **ipv6 nd suppress-ra**. This step is included in the example below.

Examples To set the advertisement lifetime of 8000 seconds on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisement lifetime to the default on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd ra-lifetime
```

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. Setting this value to 0 indicates an unspecified reachable-time.

Default 0 milliseconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Example To set the reachable-time in router advertisements on eth1 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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><milliseconds></code>	Time period in milliseconds. Valid values are from 1000 to 3600000.

Default 1000 milliseconds (1 second)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the retransmission-time of Neighbor Solicitation on eth1 to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on eth1 to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 [ipv6 nd suppress-ra](#)
commands [ipv6 nd prefix](#)

ipv6 nd route-information

Overview Use this command to supply more specific route information to be included in the RA (Router Advertisement) the device sends to downstream devices on the same link/LAN.

Use the **no** variant of this command to remove some or all route information.

Syntax `ipv6 nd route-information <ipv6-prefix/length> [<0-4294967295>|infinity|default] [low|medium|high]`
`ipv6 nd route-information <ipv6-prefix/length>`
`no ipv6 nd route-information <ipv6-prefix/length>`
`no ipv6 nd route-information all`

Parameter	Description
<code><ipv6-prefix/length></code>	The IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/ M, e.g. 2001:db8::/64
<code><0-4294967295> infinity default</code>	The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for route determination. - infinity - specifies that the route advertisement has an infinite lifetime. - default - is 3 * MaxRtrAdvInterval
<code>low medium high</code>	The preference value for the route information

Default No route information option is included in router advertisement on any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To configure a route of 2001:DB8:1::/48 on eth1.1, with a lifetime of 6000 seconds and a high preference, use the commands:

```
awplus# configure terminal
awplus(config)# int eth1.1
awplus(config-if)# ipv6 nd route-information 2001:DB8:1::/48
6000 high
```

Related commands [ipv6 nd suppress-ra](#)

Command changes Version 5.5.0-2.4: command added

ipv6 nd router-preference

Overview Use this command to set the default router preference in the router advertisements sent on a particular interface. You can use this setting to decide whether devices will use this router instead of an alternative router, by giving this router and the alternative router different values.

Use the **no** variant of this command to return the router preference to its default value.

Syntax `ipv6 nd router-preference {low|medium|high}`
`no ipv6 nd router-preference`

Parameter	Description
low	(0b11) Preference for this router on this interface is low.
medium	(0b00) Preference for this router on this interface is medium.
high	(0b01) Preference for this router on this interface is high.

Default Medium

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To set the router preference to high on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd router-preference high
```

Related commands [ipv6 nd suppress-ra](#)
[show ipv6 interface](#)

Command changes Version 5.5.1-0.1: command added

ipv6 nd suppress-ra

Overview Use this command to inhibit IPv6 Router Advertisement (RA) transmission for the current interface. Router advertisements are used when applying IPv6 stateless auto-configuration.

Use the **no** parameter with this command to enable Router Advertisement transmission.

Syntax `ipv6 nd suppress-ra`
`no ipv6 nd suppress-ra`

Default Router Advertisement (RA) transmission is suppressed by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To enable the transmission of router advertisements from eth1 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 router-preference](#)
[ipv6 nd prefix](#)

ipv6 opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global IPv6 ND cache. Opportunistic neighbor discovery changes the behavior for unsolicited ICMPv6 ND packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global IPv6 ND cache.

Syntax `ipv6 opportunistic-nd`
`no ipv6 opportunistic-nd`

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage notes When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

Related commands [arp opportunistic-nd](#)
[show ipv6 neighbors](#)
[show running-config interface](#)

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax `ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>] [description <description>]`
`no ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>]`

Parameter	Description
<i><dest-prefix/length></i>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><gateway-ip></i>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<i><gateway-name></i>	Specifies the name of the interface for the gateway (or next hop).
<i><src-prefix/length></i>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><distvalue></i>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description <i><description></i>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

**Related
Commands** [show running-config](#)
[show ipv6 route](#)

**Command
changes** Version 5.5.1-2.1: **description** parameter added
Version 5.5.0-0.3: **src-prefix** parameter added

ipv6 route vrf

Overview Use this command to add a static route to the Routing Information Base (RIB) for a VRF instance. 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.

Use the **no** variant of this command to remove the static route from the RIB and FIB.

Syntax `ipv6 route vrf <vrf-name> <dest-prefix/length> [<src-prefix/length> {<gateway-ip>|<gateway-name>}][<1-255>] [description <description>]`
`no ipv6 route vrf <vrf-name> <dest-prefix/length> [<src-prefix/length>] {<gateway-ip>|<gateway-name>}`

Parameter	Description
<vrf-name>	The name of the VRF instance.
<dest-prefix/length>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X:X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the interface for the gateway (or next hop).
<src-prefix/length>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<1-255>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description <description>	An optional description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Default Not set.

Mode Global Configuration

Usage notes You can optionally specify a description for this route, to record its purpose. The description only appears in the output of **show running-configuration** and is stored into the startup configuration. The description plays no part in routing or forwarding decisions made by the device; it is purely a textual string to aid in configuration of the device.

Example To configure an IPv6 route for the prefix 2001:0db8::1/64, with a nexthop value of vlan1 and administrative distance of 32 on VRF red, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32
```

To delete the previous route, use the command:

```
awplus(config)# no ipv6 route vrf red 2001:0db8::1/64 vlan1
```

To configure a route with a description, use the command:

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32  
description Route to head office
```

To remove a description on a route, re-enter the route without specifying the description parameter:

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32
```

Related commands [show running-config vrf](#)
[show ipv6 route](#)

Command changes Version 5.5.3-1.1: command added

ipv6 unreachables

Overview Use this command to enable ICMPv6 (Internet Control Message Protocol version 6) type 1, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax `ipv6 unreachables`
`no ipv6 unreachables`

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage notes When a device receives a packet for a destination that is unreachable it returns an ICMPv6 type 1 message. This message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ipv6 unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMPv6 destination unreachable messages breaks applications such as traceroute, which depend on these messages to operate correctly.*

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
```


ping ipv6

Overview This command sends a query to another IPv6 host (send Echo Request messages).

Syntax ping ipv6 {<host>|<ipv6-address>} [repeat {<1-2147483647>|continuous}] [size <10-1452>] [interface <interface-list>] [timeout <1-65535>]

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
size <10-1452>	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
interface <interface-list>	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet. The interface can be one of: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. You can only specify the interface when pinging a link local address.
timeout <1-65535>	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping.
size <10-1452>	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).

Parameter	Description
timeout <1-65535>	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example awplus# ping ipv6 2001:0db8::a2

Related commands [traceroute ipv6](#)

show ipv6 forwarding

Overview Use this command to display IPv6 forwarding status.

Syntax show ipv6 forwarding

Mode User Exec and Privileged Exec

Example awplus# show ipv6 forwarding

Output The following shows typical output.

Example output from the show ipv6 forwarding command

```
awplus#show ipv6 forwarding
ipv6 forwarding is on
```

show ipv6 interface

Overview Use this command to display brief information about interfaces and the IPv6 address assigned to them.

Syntax `show ipv6 interface [brief|<interface-list>] [nd]`

Parameter	Description
brief	Specify this optional parameter to display brief IPv6 interface information.
<interface-list>	The interfaces to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth1) • an 802.1Q Ethernet sub-interface (e.g. eth1.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • a WWAN interface (e.g. wwan0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4) • a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list. The specified interfaces must exist.
nd	Specify this optional parameter for Neighbor Discovery configurations.

Mode User Exec and Privileged Exec

Examples To display a brief list of all interfaces on a device, use the following command:

```
awplus# show ipv6 interface brief
```

Output The following shows typical output.

Example output from the show ipv6 interface brief command

awplus#show ipv6 interface brief			
Interface	IPv6-Address	Status	Protocol
eth1	unassigned	admin up	running
eth1.1	2001:db8::1/48	admin up	down
lo	fe80::215:77ff:fee9:5c50/64	admin up	running

Related commands [ipv6 nd router-preference](#)
[show interface brief](#)

show ipv6 neighbors

Overview Use this command to display all IPv6 neighbors.

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

Syntax show ipv6 neighbors

Mode User Exec and Privileged Exec

Example To display a device’s IPv6 neighbors, use the following command:

```
awplus# show ipv6 neighbors
```

Output The following shows typical output.

Example output of the show ipv6 neighbors command

IPv6 Address	MAC Address	Interface	Port	Type
fe80::290:bff:fe3e:44dc	0090.0b3e.44dc	eth1	-	dynamic
fd32:b1f0:dff7:ab03::1	0090.0b3e.44dc	eth1	-	dynamic
...				

Related commands [clear ipv6 neighbors](#)

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

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

Syntax `show ipv6 route [connected|database|static|summary|<ipv6-address>|<ipv6-prefix/prefix-length>]`

Syntax (VRF-lite) `show ip route [vrf <vrf-name>|global] [connected|database|static]`

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
connected	Displays only the routes learned from connected interfaces.
database	Displays only the IPv6 routing information extracted from the database.
static	Displays only the IPv6 static routes you have configured.
summary	Displays summary information from the IPv6 routing table.
<ipv6-address>	Displays the routes for the specified address in the IPv6 routing table.
<ipv6-prefix>/<prefix-length>	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output The following shows typical output.

Example output of the show ipv6 route command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0/64 via ::, eth1
...
```

Output The following shows typical output.

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
```

Example (VRF-lite) To display all IPv6 routes associated with VRF instance RED, use the command:

```
awplus# show ipv6 route vrf RED
```

Output The following shows typical output.

Example output from the show ipv6 route vrf RED command:

```
[VRF: RED]
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
       i - IS-IS, L1 - IS-IS level 1, L2 - IS-IS level 2, ia - IS-IS inter area

B   2001:172:168::/64 [20/0] via 2001:172:168:8::2, vlan10, 01:03:03
      [20/0] via 2001:172:168:10::2, vlan20, 01:03:03
C   2001:172:168:8::/64 is directly connected, vlan10
C   2001:172:168:10::/64 is directly connected, vlan20
C   fe80::/64 is directly connected, vlan10
```

Related commands [ipv6 address](#)
[ipv6 route](#)

Command changes Version 5.5.5-0.2: VRF-lite support added.

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 The following shows typical output.

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><ipv6-addr></code>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<code><hostname></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](#)

19

Routing Commands

- Contents**
- **Introduction** on page 858
 - **ip route** on page 859
 - **ipv6 route** on page 863
 - **ipv6 route vrf** on page 865
 - **max-fib-routes** on page 868
 - **max-static-routes** on page 870
 - **maximum-paths** on page 871
 - **show ip route** on page 872
 - **show ip route database** on page 875
 - **show ip route summary** on page 877
 - **show ipv6 route** on page 879
 - **show ipv6 route summary** on page 882

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](#).

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>]
[weight <1-255>] [description <description>]
no ip route <subnet&mask> {<gateway-ip>|<interface>}
[<distance>] [weight <1-255>]`

Parameter	Description
<code><subnet&mask></code>	The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats: - The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation. - The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length.
<code><gateway-ip></code>	The IPv4 address of the gateway device.
<code><interface></code>	The interface that connects your device to the network. For a VLAN, 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 switch. The gateway IP address or the interface is required if VRF-lite is not configured. If VRF-lite is configured: When adding a static intra-VRF route, you must specify either the gateway IP address or the interface. When adding a static inter-VRF route, you must specify both the gateway IP address and the interface.
<code><distance></code>	The administrative distance for the static route in the range 1 to 255. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.
weight <code><1-255></code>	Weight is used for the Weighted Lottery Load Balancing mode. See the Usage notes section for more information.
description <code><description></code>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration.

Mode Global Configuration

Default The default administrative distance for a static route is 1.

Usage notes You can use administrative distance to determine which routes take priority over other routes.

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.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

The **weight** parameter lets you assign a weight to the interface. AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

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
```

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, and a weight of 7, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
weight 7
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2
```

Related commands [ip route vrf](#)
[show ip route](#)
[show ip route database](#)

Command changes Version 5.5.1-2.1: **weight** and **description** parameters added.
Version 5.5.2-2.1: **weight** parameter added for 10GbE UTM firewall.

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax `ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>] [description <description>]`
`no ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>]`

Parameter	Description
<i><dest-prefix/length></i>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><gateway-ip></i>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<i><gateway-name></i>	Specifies the name of the interface for the gateway (or next hop).
<i><src-prefix/length></i>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><distvalue></i>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description <i><description></i>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

**Related
Commands** [show running-config](#)
[show ipv6 route](#)

**Command
changes** Version 5.5.1-2.1: **description** parameter added
Version 5.5.0-0.3: **src-prefix** parameter added

ipv6 route vrf

Overview Use this command to add a static route to the Routing Information Base (RIB) for a VRF instance. 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.

Use the **no** variant of this command to remove the static route from the RIB and FIB.

Syntax `ipv6 route vrf <vrf-name> <dest-prefix/length> [<src-prefix/length> {<gateway-ip>|<gateway-name>}][<1-255>] [description <description>]`
`no ipv6 route vrf <vrf-name> <dest-prefix/length> [<src-prefix/length>] {<gateway-ip>|<gateway-name>}`

Parameter	Description
<vrf-name>	The name of the VRF instance.
<dest-prefix/length>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X:X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the interface for the gateway (or next hop).
<src-prefix/length>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<1-255>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description <description>	An optional description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Default Not set.

Mode Global Configuration

Usage notes You can optionally specify a description for this route, to record its purpose. The description only appears in the output of **show running-configuration** and is stored into the startup configuration. The description plays no part in routing or forwarding decisions made by the device; it is purely a textual string to aid in configuration of the device.

Example To configure an IPv6 route for the prefix 2001:0db8::1/64, with a nexthop value of vlan1 and administrative distance of 32 on VRF red, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32
```

To delete the previous route, use the command:

```
awplus(config)# no ipv6 route vrf red 2001:0db8::1/64 vlan1
```

To configure a route with a description, use the command:

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32  
description Route to head office
```

To remove a description on a route, re-enter the route without specifying the description parameter:

```
awplus(config)# ipv6 route vrf red 2001:0db8::1/64 vlan1 32
```

Related commands [show running-config vrf](#)
[show ipv6 route](#)

Command changes Version 5.5.3-1.1: command added

max-fib-routes

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

NOTE:

*When using VRF-lite, this command applies to the Global VRF instance; to set the max-fib-routes for a user-defined VRF instance use the **max-fib-routes (VRF)** command. For static routes use the **max-static-routes** command for the Global VRF instance and the **max-static-routes (VRF)** command for a user-defined VRF instance.*

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

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

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

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

Mode Global Configuration

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

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

Related commands [max-fib-routes \(VRF\)](#)

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 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 commands:

```
awplus# configure terminal
awplus(config)# maximum-paths 5
```

To set the maximum paths for a route to the default of 4, use the commands:

```
awplus# configure terminal
awplus(config)# no maximum-paths
```

Command changes Version 5.5.2-2.2: command added to x330 and GS970EMX series

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.

VRF-lite If VRF-lite is configured, you can display routing entries in the FIB associated with either the global routing domain or a named VRF.

Syntax `show ip route [connected|static|<ip-addr>|<ip-addr/prefix-length>]`

Syntax (VRF-lite) `show ip route {vrf <vrf-name>|global} [connected|static]`

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
connected	Displays only the routes learned from connected interfaces.
static	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Examples To display the static routes in the FIB, use the command:
`awplus# show ip route static`

Example (VRF-lite) To display all routing entries in the FIB associated with a VRF instance red, use the command:

```
awplus# show ip route vrf red
```

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

Example output from the show ip route command

```
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - 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

Gateway of last resort is 10.37.179.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.37.179.1, eth1.179 weight 1
C     10.37.179.0/27 is directly connected, eth1.179
...
```

Connected Route An example of a 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.

Weight for Static Route If the **weight** parameter has been set using the **ip route** command, it will be shown in the output:

```
S          10.10.37.0/24 [110/11] via 10.10.31.16, eth1 weight 5
                                     via 10.10.31.32, eth1 weight 1
```

AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

Related commands

- [ip route](#)
- [ip route vrf](#)
- [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]

Syntax (VRF-lite) show ip route [vrf <vrf-name>|global] database [connected|static]

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
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 The following shows typical output.

Example output from the show ip route database command:

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth1, 00:19:21
O    10.10.31.0/24 [110/1] is directly connected, eth1, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth1
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth1
O    10.10.34.0/24 [110/31] via 10.10.31.16, eth1, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth1, 00:21:19
C    *> 10.30.0.0/24 is directly connected, eth1
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth1
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth1, 00:19:21
O    16.16.16.16/32 [110/11] via 10.10.31.16, eth1, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth1
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth1, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth1, 00:21:19
C    *> 127.0.0.0/8 is directly connected, lo
```

Example (VRF-lite) To display all routing entries in the RIB associated with a VRF instance red, use the command:

```
awplus# show ip route vrf red database
```

Output The following shows typical output.

Example output from the show ip route vrf red database command

```
[VRF: red]
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

O    192.168.10.0/24 [110/1] is directly connected, eth1, 06:45:51
C    *> 192.168.10.0/24 is directly connected, eth1
B    > 192.168.33.0/24 [20/0] via 192.168.30.3, 06:45:52
O E2 *> 192.168.110.0/24 [110/20] via 192.168.10.2, eth1, 06:45:00
O E2 *> 192.168.111.0/24 [110/20] via 192.168.10.2, eth1, 06:45:00
```

The routes added to the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the * nor the > symbol.

Related commands [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

Syntax (VRF-lite) show ip route summary [vrf <vrf-name>|global]

Parameter	Description
vrf	Specific VRF instance.
<vrf-name>	The name of the VRF instance.
global	The global routing and forwarding table.

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 The following shows typical output.

Example output from the show ip route summary command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         5
Total             5
```

Example (VRF-lite) To display a summary of the current RIB entries associated with a VRF instance red, use the command:

```
awplus# show ip route summary vrf red
```

Output The following shows typical output.

Example output from the show ip route summary vrf red command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         1
Total             1
FIB               0

[VRF: red]
Route Source      Networks
connected         1
Total             1
```

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-prefix/prefix-length>]`

Syntax (VRF-lite) `show ip route [vrf <vrf-name>|global] [connected|database|static]`

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
connected	Displays only the routes learned from connected interfaces.
database	Displays only the IPv6 routing information extracted from the database.
static	Displays only the IPv6 static routes you have configured.
summary	Displays summary information from the IPv6 routing table.
<ipv6-address>	Displays the routes for the specified address in the IPv6 routing table.
<ipv6-prefix>/<prefix-length>	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output The following shows typical output.

Example output of the show ipv6 route command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0/64 via ::, eth1
...
```

Output The following shows typical output.

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
```

Example (VRF-lite) To display all IPv6 routes associated with VRF instance RED, use the command:

```
awplus# show ipv6 route vrf RED
```

Output The following shows typical output.

Example output from the show ipv6 route vrf RED command:

```
[VRF: RED]
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
       i - IS-IS, L1 - IS-IS level 1, L2 - IS-IS level 2, ia - IS-IS inter area

B   2001:172:168::/64 [20/0] via 2001:172:168:8::2, vlan10, 01:03:03
      [20/0] via 2001:172:168:10::2, vlan20, 01:03:03
C   2001:172:168:8::/64 is directly connected, vlan10
C   2001:172:168:10::/64 is directly connected, vlan20
C   fe80::/64 is directly connected, vlan10
```

Related commands [ipv6 address](#)
[ipv6 route](#)

Command changes Version 5.5.5-0.2: VRF-lite support added.

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 The following shows typical output.

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](#)

20

VRF-lite Commands

- Contents**
- **Introduction** on page 885
 - **arp** on page 886
 - **arp opportunistic-nd** on page 888
 - **clear arp-cache** on page 890
 - **crypto key pubkey-chain knownhosts** on page 892
 - **description (VRF)** on page 894
 - **export map** on page 895
 - **http client vrf** on page 896
 - **http vrf** on page 897
 - **import map** on page 898
 - **ip route static inter-vrf** on page 899
 - **ip route vrf** on page 900
 - **ip tftp vrf** on page 904
 - **ip vrf** on page 905
 - **ip vrf forwarding** on page 906
 - **log host** on page 907
 - **log host exclude** on page 909
 - **log host (filter)** on page 914
 - **log host time** on page 919
 - **max-fib-routes (VRF)** on page 922
 - **max-static-routes (VRF)** on page 924
 - **ping** on page 925
 - **radius-server host** on page 928
 - **show arp** on page 933
 - **show crypto key pubkey-chain knownhosts** on page 936
 - **show http client** on page 938
 - **show ip interface vrf** on page 939
 - **show ip route** on page 941
 - **show ip route database** on page 944
 - **show ip route summary** on page 946
 - **show ip vrf** on page 948
 - **show ip vrf detail** on page 949
 - **show ip vrf interface** on page 950
 - **show running-config vrf** on page 951
 - **snmp-server host** on page 952
 - **snmp-server vrf** on page 955
 - **ssh** on page 956

- **ssh client** on page 959
- **ssh client vrf** on page 962
- **ssh server vrf** on page 963
- **tacacs-server host** on page 964
- **tcpdump** on page 967
- **telnet** on page 968
- **traceroute** on page 970
- **vrf** on page 971

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Virtual Routing and Forwarding Lite (VRF-lite). See the **VRF Lite Feature Overview and Configuration Guide** for more information and examples.

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.

If VRF-lite is configured, you can add ARP entries to either the global cache or for a specific VRF instance.

The **no** variant of this command removes the static ARP entry. Use the **clear arp-cache** to remove the dynamic ARP entries in the ARP cache.

Syntax `arp <ip-addr> <mac-address> [alias]`
`no arp <ip-addr>`

Syntax (VRF-lite) `arp [vrf <vrf-name>] <ip-addr> <mac-address> [<port-number>]`
`[alias]`
`no arp [vrf <vrf-name>] <ip-addr>`

Parameter	Description
<code><ip-addr></code>	The IPv4 address of the device you are adding as a static ARP entry.
<code><mac-address></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>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.
<code>vrf</code>	Apply this command to a VRF instance.
<code><vrf-name></code>	The name of the VRF instance.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4566 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2533.4566 alias
```

Example (VRF-lite) To apply the above example within a VRF instance called red use the following commands:

```
awplus# configure terminal
awplus(config)# arp vrf red 10.10.10.9 0010.2533.4566 alias
```

Related commands **clear arp-cache**
ip proxy-arp
show arp

Command changes Version 5.4.6-2.1: VRF-lite support added.

arp opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global ARP cache. This command changes the behavior for unsolicited ARP packet forwarding on the device.



CAUTION: *Opportunistic neighbor discovery can make your device more vulnerable to ARP/ND cache poisoning attacks. We recommend disabling it unless necessary.*

When using VRF-lite, you can use this command to enable opportunistic neighbor discovery for a named VRF instance.

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

Syntax (VRF-lite) arp opportunistic-nd [vrf <vrf-name>]
no arp opportunistic-nd [vrf <vrf-name>]

Parameter	Description
vrf	Apply this command to a VRF instance.
<vrf-name>	The name of the VRF instance.

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.

Note this command enables or disables opportunistic neighbor discovery for a VRF instance if the **vrf** parameter and an instance name are applied. If a VRF instance is not specified, then opportunistic neighbor discovery is enabled or disabled for device ports configured for IPv4.

Examples To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

Example (VRF-lite) To enable opportunistic neighbor discovery for the VRF instance 'blue', enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd vrf blue
```

To disable opportunistic neighbor discovery for the VRF instance 'blue', enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd vrf blue
```

Related commands **ipv6 opportunistic-nd**
show arp
show running-config interface

Command changes Version 5.4.6-2.1: VRF-lite support added.

clear arp-cache

Overview This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

When running VRF-lite, this command deletes dynamic ARP entries either from the ARP cache of a specific VRF instance, or from the ARP cache of the Global VRF instance. To delete all ARP entries from both the Global VRF instance and all VRF instances, use the command with no parameters. You can optionally specify the IPv4 address for the VRF instance to clear an ARP entry from the ARP cache.

Syntax `clear arp-cache [<ip-address>]`

Syntax (VRF-lite) `clear arp-cache [vrf <vrf-name>|global] [<ip-address>]`

Parameter	Description
<ip-address>	Specifies a specific IPv4 address for a VRF instance whose entries are to be cleared from the ARP cache.
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.
vrf	Apply this command to the specified VRF instance.
<vrf-name>	The VRF instance name.

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
```

Example (VRF-lite) To clear the dynamic ARP entries from the VRF instance named blue, use the commands:

```
awplus# clear arp-cache vrf blue
```

To clear the dynamic ARP entries from the VRF instance named blue with the IPv4 address 192.168.1.1, use the commands:

```
awplus# clear arp-cache vrf blue 192.168.1.1
```

When running VRF-lite, to clear the dynamic ARP entries from the global VRF-lite and all VRF instances, use the command:

```
awplus# clear arp-cache
```

Related commands **arp**
show arp

crypto key pubkey-chain knownhosts

Overview This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

Syntax `crypto key pubkey-chain knownhosts [ip|ipv6] <hostname> [ecdsa|rsa]`

`no crypto key pubkey-chain knownhosts <1-65535>`

Syntax (VRF-lite) `crypto key pubkey-chain knownhosts [vrf <vrf-name>] [ip|ipv6] <hostname> [ecdsa|rsa]`

`no crypto key pubkey-chain knownhosts [vrf <vrf-name>] <1-65535>`

Parameter	Description
<code>vrf</code>	Apply this command to the specified VRF instance.
<code><vrf-name></code>	The VRF instance name
<code>ip</code>	Keyword used prior to specifying an IPv4 address
<code>ipv6</code>	Keyword used prior to specifying an IPv6 address
<code><hostname></code>	IPv4/IPv6 address or hostname of a remote server in the format a.b.c.d for an IPv4 address, or in the format x:x::x:x for an IPv6 address.
<code>ecdsa</code>	Specify the ECDSA public key of the server to be added to the known host database.
<code>rsa</code>	Specify the RSA public key of the server to be added to the known host database.
<code><1-65535></code>	Specify a key identifier when removing a key using the no parameter.

Default If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

Mode Privilege Exec

Usage notes This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

Examples To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

Examples (VRF-lite) To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 in VRF 'red' to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts vrf red 192.0.2.11
```

To delete the second entry in the known host database in VRF 'red', use the command:

```
awplus# no crypto key pubkey-chain knownhosts vrf red 2
```

Validation **show crypto key pubkey-chain knownhosts**
Commands

Command changes Version 5.4.6-2.1: VRF-lite support added.

description (VRF)

Overview Use this command to add text that describes a specific VRF instance. Descriptions can be up to 80 characters long.

The **no** variant of this command removes the description of the selected VRF instance.

Syntax `description <descriptive-text>`
`no description`

Parameter	Description
<code><descriptive-text></code>	A string of up to 80 characters that describes the VRF instance.

Mode VRF Configuration

Example To add the description for a VRF instance named blue, use the following commands:

```
awplus# config terminal
awplus(config)# ip vrf blue
awplus(config-vrf)# description the text description of vrf blue
```

Related commands [show ip vrf](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

export map

Overview This command associates a route map with a specific VRF instance. It provides a finer control over the routes that are exported out of a VRF instance by the **route-target** command. Note, however, that this command does not replace the need for a route-target export in the VRF configuration.

The **no** variant of this command disables the capability to export route map entries for a specified VRF instance.

Syntax export map <route-map>
no export map

Parameter	Description
<route-map>	The route-map name.

Mode VRF Configuration

Usage notes Use this command to export route-map entries in VRF configuration mode.

Example To export the route map named routemap2 for the VRF instance named blue, use the following commands:

```
awplus# config terminal
awplus(config)# ip vrf blue
awplus(config-vrf)# export map routemap2
```

Related commands [import map](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

http client vrf

Overview Use this command to enable the use of a specific VRF for the command `copy http`.

Use the **no** variant of this command to disable the configured VRF.

Syntax `http client vrf <vrf-name>`
`no http client vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when copying a file using HTTP.

Default Global VRF.

Mode Privileged Exec

Examples To enable the use of VRF 'MyVRF', use the commands:

```
awplus# configure terminal
awplus(config)# http client vrf MyVRF
```

To remove a specified VRF and revert to the global VRF, use the commands:

```
awplus# configure terminal
awplus(config)# no http client vrf
```

Output The following shows typical output.

Example output if the specified VRF does not exist:

```
"Invalid VRF instance MyVRF"
```

Related commands [copy \(filename\)](#)
[show http client](#)

Command changes Version 5.5.2-1.1: command added

http vrf

Overview Use this command to configure an HTTP server to be run within a specified VRF.

Use the **no** variant of this command to remove a VRF configuration from the HTTP server.

Syntax `http vrf <vrf-name>`
`no http vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when running the HTTP server. The name of the VRF instance.

Default By default the HTTP server uses the global VRF.

Mode Global Configuration

Examples To configure VRF 'MyVRF', use the commands:

```
awplus# configure terminal
awplus(config)# http vrf MyVRF
```

To return the HTTP server to the global VRF, use the commands:

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

Related commands [service http](#)
[show http](#)

Command changes Version 5.5.2-1.1: command added

import map

Overview The import map command associates a route map with a specific VRF instance. The import map command does not replace the need for a route-target import in the VRF configuration. It provides a finer control over the routes imported into a VRF instance by the **route-target** command.

The **no** variant of this command disables the capability to import route map entries for a specified VRF instance.

Syntax `import map <route-map>`
`no import map`

Parameter	Description
<code><route-map></code>	The route-map name.

Mode VRF Configuration

Usage notes Use this command to import route-map entries into the specified VRF instance.

Example To import the route map named routemap2 for the VRF instance named blue, use the following commands:

```
awplus# config terminal
awplus(config)# ip vrf blue
awplus(config-vrf)# import map routemap2
```

Related commands [export map](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

ip route static inter-vrf

Overview Applying this command enables static inter-VRF routing. Note that static inter-VRF routing must be enabled before you can use the **ip route** command to create a static inter-VRF route.

The **no** variant of this command disables static inter-VRF routing.

Syntax `ip route static inter-vrf`
`no ip route static inter-vrf`

Mode VRF Configuration

Default Static inter-VRF routing is enabled.

Example To enable static inter-VRF routing, use the following commands:

```
awplus# config terminal
awplus(config)# ip route static inter-vrf
```

Related commands [ip route](#)
[show ip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

ip route vrf

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.

When using VRF (Virtual Routing and Forwarding), you can use this command to configure a static inter-VRF route to a destination network that is reachable by a remote gateway located in a different VRF instance. Note that to apply the command in this way, the **ip route static inter-vrf** command must be in enabled (its default condition). For more information about VRF, see the **VRF Feature Overview and Configuration Guide** and **VRF-lite Commands**.

The **no** variant of this command removes the static route from the RIB and FIB.

Syntax `ip route [vrf <vrf-name>] <subnet&mask> {<gateway-ip>|<interface>} [<distance>] [weight <1-255>] [description <description>]`
`no ip route [vrf <vrf-name>] <subnet&mask> {<gateway-ip>|<interface>} [<distance>] [weight <1-255>]`

Parameter	Description
<code><subnet&mask></code>	The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats: - The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation. - The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length.
<code><gateway-ip></code>	The IPv4 address of the gateway device.
<code><interface></code>	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 switch. The gateway IP address or the interface is required if VRF-lite is not configured. If VRF-lite is configured: When adding a static intra-VRF route, you must specify either the gateway IP address or the interface. When adding a static inter-VRF route, you must specify both the gateway IP address and the interface.
<code><distance></code>	The administrative distance for the static route in the range 1 to 255. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.
<code>vrf</code>	Applies the command to the specified VRF instance.
<code><vrf-name></code>	The name of the VRF instance to enter IPv4 Address-Family mode for.
<code>weight <1-255></code>	Weight is used for the Weighted Lottery Load Balancing mode. See the Usage notes section for more information.
<code>description</code> <code><description></code>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Default The default administrative distance for a static route is 1.

Usage notes You can use administrative distance to determine which routes take priority over other routes.

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.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

The **weight** parameter lets you assign a weight to the interface. AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

Examples To create a static route from source VRF instance red, to the subnet 192.168.50.0/24 with a next hop of 192.168.20.6, use the following commands:

```
awplus# configure terminal
awplus(config)# ip route vrf red 192.168.50.0/24 192.168.20.6
```

To remove a static route from source VRF red, to the subnet 192.168.50.0/24 with a next hop of 192.168.20.6, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip route vrf red 192.168.50.0/24 192.168.20.6
```

To create a static route from source VRF red, to the subnet 192.168.50.0/24 with a next hop of 192.168.20.6 via vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip route vrf red 192.168.50.0/24 192.168.20.6
vlan10
```

To create a static route from source VRF instance red, to the subnet 192.168.50.0/24 with a next hop of 192.168.20.6, and a weight of 7, use the following commands:

```
awplus# configure terminal
awplus(config)# ip route vrf red 192.168.50.0/24 192.168.20.6
weight 7
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ip route vrf red 192.168.50.0/24 192.168.20.6
description test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ip route vrf red 192.168.50.0/24 192.168.20.6
```

Related commands [ip route](#)
[show ip route](#)
[show ip route database](#)

Command changes Version 5.5.2-1.1: **fall-over bfd** and **profile** parameters added for the SBx81CFC960, SBx908 GEN2, x950, x930, and x530 series.

Version 5.5.1-2.1: **weight** and **description** parameters added.

Version 5.5.2-2.1: **weight** parameter added for 10GbE UTM firewall.

ip tftp vrf

Overview Use this command to specify a VRF to use when copying a file via TFTP. Use the **no** variant of this command to remove the VRF from the configuration and set it back to the default VRF.

Syntax `ip tftp vrf <vrf-name>`
`no ip tftp vrf`

Parameter	Description
<code>vrf <vrf-name></code>	Specify the VRF to use when copying a file using TFTP.

Default Global VRF

Mode Global Configuration

Example To configure a VRF called 'red' to use when copying a file via TFTP, use the commands:

```
awplus# configure terminal
awplus(config)# ip tftp vrf red
```

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

Command changes Version 5.5.2-1.1: command added

ip vrf

Overview This command creates a VRF instance and specifies its unique name. You can also optionally specify a VRF ID. If you do not specify the VRF ID, a unique ID will automatically be created and assigned to the VRF instance.

The **no** variant of this command removes a selected VRF instance. All interfaces previously belonging to the removed instance are then returned to the global routing and forwarding environment.

Syntax `ip vrf <vrf-name> [<vrf-inst-id>]`
`no ip vrf <vrf-name> [<vrf-inst-id>]`

Parameter	Description
<code><vrf-name></code>	The name of the VRF instance.
<code><vrf-inst-id></code>	The ID of the VRF instance, a number in the range 1 to 8.

Mode Global Configuration

Default Static inter-VRF routing is enabled

Example To create a VRF instance named `vrf blue` and assign it the ID number 2, use the following commands:

```
awplus# config terminal
awplus(config)# ip vrf blue 2
```

Command changes Version 5.4.6-2.1: On AR Series devices: VRF-lite support added

Version 5.5.0-0.1: On SBx908 GEN2 and x950 Series devices: **vrf-inst-id** parameter range increased to 600.

ip vrf forwarding

Overview This command associates a VRF instance with an interface.

The **no** variant of this command disassociates the VRF instance from its interface.

Syntax `ip vrf forwarding <vrf-name>`
`no ip vrf <vrf-name>`

Parameter	Description
<vrf-name>	The name of the VRF instance.

Mode Interface Configuration

Default The default for an interface is the global routing table.

Examples For LAN interfaces, to associate the VRF instance named blue with the VLAN interface vlan-admin, use the following commands:

```
awplus# config terminal
awplus(config)# interface vlan-admin
awplus(config-if)# ip vrf forwarding blue
```

Related commands [show ip vrf](#)
[show ip vrf detail](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

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>`

Syntax (VRF-lite) `log host <ipv4-addr>|<ipv6-addr> [vrf <vrf-name>] [secure]`
`no log host <ipv4-addr>|<ipv6-addr> [vrf <vrf-name>]`

Parameter	Description
<code><ipv4-addr></code>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<code><ipv6-addr></code>	Specify the source IPv6 address, in X:X::X:X notation.
<code>vrf <vrf-name></code>	The name of a VRF instance. Use this to specify the VRF that the remote syslog server (host) is accessible by. Hosts are uniquely identified by their address and VRF, so multiple hosts can have the same address as long as the VRF is different. The default is the global VRF.
<code>secure</code>	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
```

Example (VRF-lite) To configure the device to send log messages to a remote syslog server that is accessible via VRF 'red', use the following commands:

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

Related commands

- default log host**
- log host (filter)**
- log host exclude**
- log host source**
- log host startup-delay**
- log host time**
- log trustpoint**
- show log config**

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host exclude

Overview Use this command to prevent specified log messages from being sent to the remote syslog server, when **log host** is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude
[level <level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]
no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude
[level <level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]`

Syntax (VRF-lite) `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<hostname>	The host name of a remote syslog server.																
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.																
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.																
vrf <vrf-name>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.																
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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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 predefined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)						
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

Parameter	Description
	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 exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 exclude msgtext example of
irrelevant message
```

Example (VRF-lite) To exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, within VRF 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 vrf red exclude msgtext
example of irrelevant message
```

Related commands

- default log host**
- log host**
- log host (filter)**
- log host source**
- log host time**
- show log config**

Command changes Version 5.2.2-1.1: **vrf** parameter added for products that support VRF

log host (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>]`

Syntax (VRF-lite) `log host <ip-addr> [vrf <vrf-name>] [level <level>]
[program <program-name>] [facility <facility>] [msgtext <text-string>]
no log host <ip-addr> [vrf <vrf-name>] [level <level>]
[program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<code><ip-addr></code>	The IP address of a remote syslog server.																
<code>vrf <vrf-name></code>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.																
<code>level</code>	Filter messages by severity level.																
<code><level></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: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	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
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><program- name></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. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
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
poel	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
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

Parameter	Description
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:

```
awplusawplus# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Example (VRF-lite) 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, when that server is in VRF ‘red’, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 vrf red level informational
```

Related commands

- [default log host](#)
- [log host](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host time

Overview This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} time {local|local-offset|utc-offset {plus|minus} <0-24>}`

Syntax (VRF-lite) `log host {<ipv4-addr>|<ipv6-addr>} [vrf <vrf-name>] time {local|local-offset|utc-offset {plus|minus} <0-24>}`

Parameter	Description
<hostname>	The host name of a remote syslog server.
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.
<email-address>	The email address to send log messages to
vrf <vrf-name>	The name of a VRF instance. Use this if the syslog server is inside a VRF. The default is the global VRF.
time	Specify the time difference between the email recipient and the device you are configuring.
local	The device is in the same time zone as the email recipient
local-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
utc-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
plus	Negative offset (difference) from the device to the syslog server.
minus	Positive offset (difference) from the device to the syslog server.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

Examples To send messages to the remote syslog server with the IP address 10.32.16.21 in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address 10.32.16.12 with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address 10.32.16.02 with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Example (VRF-lite) To send messages to the remote syslog server with the IP address 10.32.16.02 within the VRF 'red', in the same time zone as the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 vrf red time utc-offset
minus 3
```

Related commands

- default log host**
- log host**
- log host (filter)**
- log host exclude**
- log host source**
- show log config**

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

max-fib-routes (VRF)

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

NOTE: This command applies to a user-defined VRF instance; to set the max-fib-routes for the Global VRF instance use the command. For static routes use the command for the Global VRF instance and the command for a user-defined VRF instance.

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

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

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

Mode VRF Configuration

Default Sets the maximum number of dynamic routes to 4294967294 and no warning threshold.

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

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

Related commands [max-fib-routes](#)
[show ip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

max-static-routes (VRF)

Overview Use this command to set the maximum number of static routes (excluding FIB—Forwarding Information Base routes) for VRF instances. A limit of 1000 static routes can be assigned to each individual VRF instance. For example you can assign 800 static routes to the Global VRF, then also assign 600 static routes to VRF instance Blue, and a further 600 routes to VRF instance Green.

NOTE: *This command applies to a user-defined VRF instance; to set the max-static-routes for the Global VRF instance use the command. For FIB routes use the command for the Global VRF instance and the command for a user-defined VRF instance.*

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

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

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

Mode VRF Configuration

Example To assign 200 static routes to VRF instance Blue, use the following commands:

```
awplus# configure terminal
awplus(config)# ip vrf blue
awplus(config-vrf)# max-static-routes 200
```

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 \(VRF\)](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

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>]

**Syntax (VRF-
lite)** ping [vrf <vrf-name>] [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.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

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
```

Example (VRF-lite) To ping the IP address 10.10.0.5 from VRF instance 'red', use the following command:

```
awplus# ping vrf red 10.10.0.5
```

NOTE: Unless a cross-domain static or leaked route exists to the destination IP address, you must run this command from within the same routing domain as the address being pinged.

Command changes Version 5.4.6-2.1: VRF-lite support added.

radius-server host

Overview Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [encrypted] [retransmit <0-100>] [timeout <1-1000>]
no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>]

Syntax (VRF-lite) radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [encrypted] [retransmit <0-100>] [timeout <1-1000>] [vrf <vrf-name>]
no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [vrf <vrf-name>]

Parameter	Description
<i><host-name></i>	Server host name. The DNS name of the RADIUS server host.
<i><ip-address></i>	The IP address of the RADIUS server host.
acct-port	Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.
<i><0-65535></i>	UDP port number. (Accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting.
auth-port	Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.
<i><0-65535></i>	UDP port number (authentication port number is set to 1812 by default). Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.
timeout	Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the radius-server timeout command is used.
<i><1-1000></i>	Time in seconds to wait for a server reply (timeout is set to 5 seconds by default). The time interval (in seconds to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the radius-server timeout command. If no timeout value is specified for this server, the global value is used.
retransmit	Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the radius-server retransmit command is used.
<i><0-100></i>	Maximum number of retries (maximum number of retries is set to 3 by default). The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the radius-server retransmit command. If no retransmit value is specified, the global value is used.

Parameter	Description
key	Set shared secret key with RADIUS servers.
<key-string>	Shared key string applied. Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored. This setting overrides the global setting of the radius-server key command. If no key value is specified, the global value is used.
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.
vrf <vrf-name>	The name of a VRF instance. Use this to specify the VRF that the RADIUS server is accessible by. Servers are uniquely identified by their address and VRF, so multiple servers can have the same address or host-name as long as the VRF is different. The default is the global VRF.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius-server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the **auth-port** parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret
```

To delete the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure rad1.company.com for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server rad1.company.com configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com acct-port
0
```

To configure rad2.company.com for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Examples (VRF-lite) To add the RADIUS server 10.0.0.20 in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 vrf red
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20 in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret vrf
red
```

Related commands **aaa group server**
 radius-server key
 radius-server retransmit
 radius-server timeout

Command changes Version 5.5.3-2.1: **encrypted** parameter added
 Version 5.5.2-1.1: **vrf** parameter added for products that support VRF
 Version 5.4.9-2.1: **key-encrypted** parameter 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

Syntax (VRF-lite) show arp [global|vrf <vrf-name>]

Parameter	Description
global	When VRF-lite is configured, apply this command to the global routing and forwarding table.
vrf	Apply this command to the specified VRF instance.
<vrf-name>	The VRF instance name.

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.

With VRF-lite configured, and no additional parameters entered, the command output displays all entries, listed by their VRF instance. By adding either a specific VRF instance or global parameter entry, you can selectively list ARP entries by their membership of a specific VRF instance.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output The following shows typical output.

Example output from the show arp command

awplus#show arp					
IP Address	LL Address	Interface	Port	Type	
10.38.50.2	001a.eb9c.f367	eth1	-	dynamic	
172.31.1.211	001a.eb9c.f367	br1	-	dynamic	
10.38.50.1	000d.b957.6f9d	eth1	-	dynamic	

Example (VRF-lite) To display the dynamic ARP entries in the global routing instance, use the command:

```
awplus# show arp global
```

Output The following shows typical output.

Example output from the show arp global command

awplus#show arp global					
IP Address	LL Address	Interface	Port	Type	
192.168.10.2	0015.77ad.fad8	eth1	-	dynamic	
192.168.1.100	0015.77ad.fa48	eth2	-	static	

Example (VRF-lite) To display the dynamic ARP entries for a VRF instance 'red', use the command:

```
awplus# show arp vrf red
```

Output The following shows typical output.

Example output from the show arp vrf red command

awplus# show arp vrf red					
[VRF: red]					
IP Address	LL Address	Interface	Port	Type	
192.168.10.2	0015.77ad.fad8	eth1	-	dynamic	

Parameters in the output of the show arp command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
LL Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the arp command. Dynamic entries are learned from ARP request/reply message exchanges.
VRF	The name of the VRF instance. The VRF-lite components only display when VRF-lite is configured.

Related commands [arp](#)
[clear arp-cache](#)
[ip vrf](#)

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 crypto key pubkey-chain knownhosts

Overview This command displays the list of public keys maintained in the known host database on the device.

Syntax show crypto key pubkey-chain knownhosts [*<1-65535>*]

Syntax (VRF-lite) show crypto key pubkey-chain knownhosts [vrf *<vrf-name>*][global] [*<1-65535>*]

Parameter	Description
global	When VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<i><vrf-name></i>	The name of the VRF instance.
<i><1-65535></i>	Key identifier for a specific key. Displays the public key of the entry if specified.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Usage When VRF-lite is configured:

- If **vrf** is specified, this command displays the known host database from the specified VRF instance.
- If **global** is specified, this command displays the known host database from the global routing environment.
- If neither **vrf** nor **global** is specified, this command displays the known host database from the global routing environment and each configured VRF.

For more information about VRF, see the [VRF Lite Feature Overview and Configuration Guide](#).

Examples To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

Output The following shows typical output.

Example output from the show crypto key public-chain knownhosts command

No	Hostname	Type	Fingerprint
1	172.16.23.1	rsa	c8:33:b1:fe:6f:d3:8c:81:4e:f7:2a:aa:a5:be:df:18
2	172.16.23.10	rsa	c4:79:86:65:ee:a0:1d:a5:6a:e8:fd:1d:d3:4e:37:bd
3	5ffe:1053:ac21:ff00:0101:bcd:f:ffff:0001	rsa1	af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57

Parameters in the output of the show crypto key public-chain knownhosts command

Parameter	Description
No	Number ID of the key.
Hostname	Host name of the known SSH server.
Type	The algorithm used to generate the key.
Fingerprint	Checksum value for the public key.

Related commands [crypto key pubkey-chain knownhosts](#)

Command changes Version 5.5.3-1.1: added to AR1050V
Version 5.4.6-2.1: VRF-lite support added for AR-Series devices

show http client

Overview Use this command to show the current HTTP client VRF.

Syntax show http client

Mode Privileged Exec

Usage notes If no VRF has been set, the show command shows 'None'.

Example To display the HTTP client VRF, use the commands:

```
awplus# show http client
```

Output The following shows typical output.

Example output from show http client

```
awplus#show http client
Hyper-Text Transfer Protocol Client Configuration
-----
VRF                                     : MyVRFPoE
```

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

Command changes Version 5.5.2-1.1: command added

show ip interface vrf

Overview Use this command to display protocol and status information about configured interfaces and their assigned IP addresses in VRF instances.

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

Syntax `show ip interface [vrf <vrf-name>|global]`

Parameter	Description
vrf	A VRF instance.
<vrf-name>	The name of a specific VRF instance.
global	The global routing and forwarding table.

Mode User Exec and Privileged Exec

Examples To display all interfaces and IP addresses associated with a VRF instance 'red', use the command:

```
awplus# show ip interface vrf red
```

Output The following shows typical output.

Example output from show ip interface vrf red

[VRF: red]			
Interface	IP-Address	Status	Protocol
lo1	unassigned	admin up	running
vlan1	192.168.10.1/24	admin up	running

Example To display all interfaces and IP addresses associated with all VRF instances, use the command:

```
awplus# show ip interface
```

Output **Example output from the show ip interface with VRF-lite configured**

Interface	IP-Address	Status	Protocol
eth0	unassigned	admin up	down
lo	unassigned	admin up	running
vlan1	192.168.1.1/24	admin up	running
vlan4	172.30.4.43/24	admin up	down
[VRF: red]			
Interface	IP-Address	Status	
Protocol			
lo1	unassigned	admin up	running
[VRF: blue]			
Interface	IP-Address	Status	
Protocol			
lo2	unassigned	admin up	running

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip route

Overview Use this command to display routing entries in the FIB (Forwarding Information Base). The FIB contains the best routes to a destination, and your device uses these routes when forwarding traffic. You can display a subset of the entries in the FIB based on protocol.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

VRF-lite If VRF-lite is configured, you can display routing entries in the FIB associated with either the global routing domain or a named VRF.

Syntax `show ip route [connected|static|<ip-addr>|<ip-addr/prefix-length>]`

Syntax (VRF-lite) `show ip route {vrf <vrf-name>|global} [connected|static]`

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
connected	Displays only the routes learned from connected interfaces.
static	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Examples To display the static routes in the FIB, use the command:
`awplus# show ip route static`

Example (VRF-lite) To display all routing entries in the FIB associated with a VRF instance red, use the command:

```
awplus# show ip route vrf red
```

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

Example output from the show ip route command

```
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       0 - 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

Gateway of last resort is 10.37.179.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.37.179.1, eth1.179 weight 1
C     10.37.179.0/27 is directly connected, eth1.179
...
```

Connected Route An example of a 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.

Weight for Static Route If the **weight** parameter has been set using the **ip route** command, it will be shown in the output:

```
S      10.10.37.0/24 [110/11] via 10.10.31.16, eth1 weight 5
                               via 10.10.31.32, eth1 weight 1
```

AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

Related commands

- [ip route](#)
- [ip route vrf](#)
- [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]

Syntax (VRF-lite) show ip route [vrf <vrf-name>|global] database [connected|static]

Parameter	Description
global	If VRF-lite is configured, apply the command to the global routing and forwarding table.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.
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 The following shows typical output.

Example output from the show ip route database command:

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth1, 00:19:21
O    10.10.31.0/24 [110/1] is directly connected, eth1, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth1
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth1
O    10.10.34.0/24 [110/31] via 10.10.31.16, eth1, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth1, 00:21:19
C    *> 10.30.0.0/24 is directly connected, eth1
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth1
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth1, 00:19:21
O    16.16.16.16/32 [110/11] via 10.10.31.16, eth1, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth1
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth1, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth1, 00:21:19
C    *> 127.0.0.0/8 is directly connected, lo
```

Example (VRF-lite) To display all routing entries in the RIB associated with a VRF instance red, use the command:

```
awplus# show ip route vrf red database
```

Output The following shows typical output.

Example output from the show ip route vrf red database command

```
[VRF: red]
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

O    192.168.10.0/24 [110/1] is directly connected, eth1, 06:45:51
C    *> 192.168.10.0/24 is directly connected, eth1
B    > 192.168.33.0/24 [20/0] via 192.168.30.3, 06:45:52
O E2 *> 192.168.110.0/24 [110/20] via 192.168.10.2, eth1, 06:45:00
O E2 *> 192.168.111.0/24 [110/20] via 192.168.10.2, eth1, 06:45:00
```

The routes added to the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the * nor the > symbol.

Related commands [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

Syntax (VRF-lite) show ip route summary [vrf <vrf-name>|global]

Parameter	Description
vrf	Specific VRF instance.
<vrf-name>	The name of the VRF instance.
global	The global routing and forwarding table.

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 The following shows typical output.

Example output from the show ip route summary command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         5
Total             5
```

Example (VRF-lite) To display a summary of the current RIB entries associated with a VRF instance red, use the command:

```
awplus# show ip route summary vrf red
```

Output The following shows typical output.

Example output from the show ip route summary vrf red command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         1
Total             1
FIB               0

[VRF: red]
Route Source      Networks
connected         1
Total             1
```

Related commands [show ip route](#)
[show ip route database](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip vrf

Overview This command displays brief configurations for a specific VRF instance.

Syntax `show ip vrf <vrf-name>`

Parameter	Description
<vrf-name>	The name of the VRF instance.

Mode User Exec and Privileged Exec

Example To display brief information for the VRF instance red, use the command:
`awplus# show ip vrf red`

Output The following shows typical output.

Example output from the show ip vrf red command

Name	Default RD	Interfaces
red	500:1	lo1, vlan1

Related commands [show ip vrf interface](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip vrf detail

Overview This command displays the detailed configuration for a specific VRF instance.

Syntax show ip vrf detail <*vrf-name*>

Parameter	Description
< <i>vrf-name</i> >	The name of the VRF instance.

Mode User Exec and Privileged Exec

Example To display the detailed information for all VRF instances, use the command:

```
awplus# show ip vrf detail
```

Output The following shows typical output.

Example output from the show ip detail command, for all VRF instances

```
VRF blue; Description: VRF for customer blue
FIB ID 3; Router ID: 192.168.30.1 (automatic)
Default RD 500:3
  Interfaces:
    lo3, vlan3
  Export route-target communities
    RT: 500:3
  Import route-target communities
    RT: 500:4
  Import route-map: blue45
  No export route-map

VRF red
FIB ID 1; Router ID: 192.168.10.1 (automatic)
Default RD 500:1
  Interfaces:
    lo1, vlan1
  Export route-target communities
    RT: 500:1
  Import route-target communities
    RT: 500:1
  Import route-map: red43
  No export route-map
```

Related commands [show ip vrf](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip vrf interface

Overview This command displays protocol, operational status, and address information, for interfaces existing within either a specified VRF instance, or all VRF instances.

Syntax show ip vrf interface <vrf-name>

Parameter	Description
<vrf-name>	The name of the VRF instance.

Mode User Exec and Privileged Exec

Example To display all interfaces and IP addresses associated with all VRF instances, use the command:

```
awplus# show ip vrf interface
```

Output The following shows typical output.

Example output from the show ip vrf interface command

Interface	IP-Address	Status	Protocol	Vrf
lo1	unassigned	admin up	running	red
lo2	unassigned	admin up	running	green
vlan1	192.168.10.1/24	admin up	running	red
vlan2	192.168.20.1/24	admin up	running	green

Example To display all interfaces and IP addresses associated with the VRF instance red, use the command:

```
awplus# show ip vrf interface red
```

Output The following shows typical output.

Example output from the show ip vrf interface red command

Interface	IP-Address	Status	Protocol	Vrf
lo1	unassigned	admin up	running	red
vlan1	192.168.10.1/24	admin up	running	red

Related commands [show ip vrf](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show running-config vrf

Overview This command displays the running system VRF-related configurations for all VRF instances.

Syntax show running-config vrf

Mode Privileged Exec

Example To display the running system VRF-related configurations, use the command:

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

Output The following shows typical output.

Example output from the show running config vrf command

```
ip vrf red
rd 500:1
route-target export 500:1
route-target export 500:4
import map red 43
!
```

Related commands [show ip vrf](#)

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).

When VRF-lite is configured, you can apply this command to a specific VRF instance.

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>`

Syntax (VRF-Lite) `snmp-server host {<ipv4-address>|<ipv6-address>} [vrf <vrf-
name>] [informs|traps] version {1|2c|3} {auth|noauth|priv}
{<community-name>|<user-name>}
no snmp-server host {<ipv4-address>|<ipv6-address>} [vrf <vrf-
name>] [informs|traps] version {1|2c|3} {auth|noauth|priv}
{<community-name>|<user-name>}`

Parameter	Description
<i><ipv4-address></i>	IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.
<i><ipv6-address></i>	IPv6 trap host address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
vrf <i><vrf-name></i>	Specify the VRF instance to use. If you do not specify an instance it will use the global VRF.
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.
auth	Authentication.
noauth	No authentication.
priv	Encryption.
<i><community-name></i>	The SNMPv1 or SNMPv2c community name.
<i><user-name></i>	SNMPv3 user name.

Default No host is defined.

Mode Global Configuration

Usage notes You can test connectivity to the host by using the command **test snmp** **trap snmp**.

Examples To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name 'private', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 2001:db8::8a2e:7334 version 2c
private
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to an IPv4 host destination 192.168.1.2 with the SNMPv2c community name 'public' and on a VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.1.2 vrf red version 2c
public
```

Related commands

- [snmp trap link-status](#)
- [snmp-server enable trap](#)
- [snmp-server view](#)
- [test snmp trap snmp](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

snmp-server vrf

Overview Use this command to isolate the SNMP Agent to operate within a previously configured non-global named VRF. This means the SNMP Agent can only respond to requests from SNMP Managers operating within the same VRF.

Use the **no** variant of this command to revert the SNMP Agent to operating within the default global VRF.

Syntax `snmp-server vrf <vrf-name>`
`no snmp-server vrf`

Parameter	Description
<code>vrf</code>	The VRF instance to operate within.
<code><vrf-name></code>	The VRF instance name.

Default Global VRF

Mode Global Configuration

Examples To configure the SNMP Agent to operate within the VRF instance named 'red', use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server vrf red
```

To revert the SNMP Agent to operating within the default global VRF, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server vrf
```

Related commands [show snmp-server](#)
[snmp-server](#)

Command changes Version 5.5.2-2.1: command added

ssh

Overview Use this command to initiate a Secure Shell connection to a remote SSH server.

If the server requests a password to login, you need to type in the correct password at the "Password:" prompt.

An SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

NOTE: A hostname specified with SSH cannot begin with a hyphen (-) character.

Syntax `ssh [ip|ipv6] [user <username>|port <1-65535>|version 2]
<remote-device> [<command>]`

Syntax (VRF-lite) `ssh vrf <vrf-name> [ip|ipv6] [user <username>|port <1-65535>|
version 2] <remote-device> [<command>]`

Parameter	Description
vrf	Apply the command to the specified VRF instance. When using VRF, specifying a VRF name means the command will apply to that VRF instance, and not specifying a VRF name means the command will apply to the global VRF.
<vrf-name>	The name of the VRF instance.
ip	Specify IPv4 SSH.
ipv6	Specify IPv6 SSH.
user	Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.
	<username> User name to login on the remote server.
port	SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Otherwise, the client port configured by "ssh client" command or the default TCP port (22) is used.
	<1-65535> TCP port.
version	SSH client version. From 5.5.1-1.1 onwards, SSH only supports version 2.
<remote-device>	IPv4/IPv6 address or hostname of a remote server. The address is in the format A.B.C.D for an IPv4 address, or in the format X:X::X:X for an IPv6 address. Note that a hostname specified with SSH cannot begin with a hyphen (-) character.
<command>	A command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.

Mode User Exec and Privileged Exec

Examples To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user 'manager', use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening on TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server 'example_host' using an IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

Example (VRF-lite) To login to the remote SSH server at 192.168.1.1 on VRF "red", use the command:

```
awplus# ssh vrf red 192.168.1.1
```

Related commands

- [crypto key generate userkey](#)
- [crypto key pubkey-chain knownhosts](#)
- [debug ssh client](#)
- [ssh client](#)

Command changes

- Version 5.5.3-1.1: added to AR1050V
- Version 5.5.1-1.1: support removed for SSH protocol v1
- Version 5.4.8-2.1: secure mode syntax added for x950, SBx908 GEN2.
- Version 5.4.8-1.2: secure mode syntax added for x220, x930, x550, XS900MX.
- Version 5.4.6-2.1: VRF-lite support added for AR-Series devices.

ssh client

Overview This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the **ssh client** command, and restores the defaults.

This command does not affect the existing SSH sessions.

Syntax `ssh client {port <1-65535>|version 2|session-timeout <0-3600>|connect-timeout <1-600>}`
`no ssh client {port|version|session-timeout|connect-timeout}`

Syntax (VRF-lite) `ssh client {port <1-65535>|version 2|session-timeout <0-3600>|connect-timeout <1-600>|vrf <vrf-name>}`
`no ssh client {port|version|session-timeout|connect-timeout|vrf}`

Parameter	Description
port	The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port. Default: 22 <1-65535> TCP port number.
version	The SSH version used by the client for SSH sessions. From 5.5.1-1.1 onwards, the SSH client supports only version 2
session-timeout	The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout. Default: 0 (session timer remains off) <0-3600> Timeout in seconds.
connect-timeout	The maximum time period that an SSH session can take to become established. The SSH client terminates the SSH session if this timeout expires and the session is still not established. Default: 30 <1-600> Timeout in seconds.
vrf <vrf-name>	The VRF to use for SSH clients. Default: the global VRF.

Mode Privileged Exec

Examples To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

Example (VRF-lite) To configure SSH clients to use the VRF named 'red', use the command:

```
awplus# ssh client vrf red
```

Related commands [show ssh client](#)
[ssh](#)

Command changes Version 5.5.3-1.1: added to AR1050V
Version 5.5.2-1.1: **vrf** parameter added for products that support VRF
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH
and for SSH protocol v1

ssh client vrf

Overview Use this command to modify the configured VRF of the SSH client. Use this configuration for any SSH client on the device to connect to remote SSH servers.

Use the **no** variant of this command to restore the configured VRF to the default VRF (global VRF).

Syntax `ssh client vrf <vrf-name>`
`no client vrf`

Parameter	Description
<code>vrf <vrf-name></code>	The name of the VRF to use for SSH clients. This overrides the default.

Default Global VRF

Mode Global Configuration

Usage notes Any VRF parameter specified on the SSH client explicitly overrides the default configuration parameters. This also affects the copy commands that utilize SSH such as **copy scp** and **copy sftp**.

This change affects all new user shell sessions. Existing sessions will not be affected.

A user may override this on a per-session basis using the executive mode variant of this command.

Examples To configure the VRF named 'management' for SSH clients, use the commands:

```
awplus# configure terminal
awplus(config)# ssh client vrf management
```

To restore to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh client vrf
```

Related commands [show ssh client](#)
[ssh client](#)

Command changes Version 5.5.2-2.1: command added

ssh server vrf

Overview Use this command to specify a VRF for the SSH server to operate within.
Use the **no** variant of this command to return the SSH server to the default VRF.

Syntax `ssh server vrf [<vrf-name>]`
`no ssh server vrf`

Parameter	Description
<vrf-name>	The name of the VRF instance

Default The global VRF

Mode Global Configuration

Example To configure the SSH server to operate within the VRF instance named 'red', use the command:

```
awplus# configure terminal
awplus(config)# ssh server vrf red
```

To return the SSH server to operating within the global VRF instance, use the command:

```
awplus# configure terminal
awplus(config)# no ssh server vrf
```

Related commands [show ssh server](#)
[ssh](#)
[ssh server](#)

Command changes Version 5.5.2-1.1: command added

tacacs-server host

Overview Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

Syntax `tacacs-server host {<host-name>|<ip-address>} [key [8|9] <key-string>]`
`no tacacs-server host {<host-name>|<ip-address>}`

Syntax (VRF-lite) `tacacs-server host {<host-name>|<ip-address>} [vrf <vrf-name>] [key [8|9] <key-string>]`
`no tacacs-server host {<host-name>|<ip-address>} [vrf <vrf-name>]`

Parameter	Description
<i><host-name></i>	Server host name. The DNS name of the TACACS+ server host.
<i><ip-address></i>	The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.
<i>vrf <vrf-name></i>	The name of a VRF instance. Use this to specify the VRF that the TACACS+ server is accessible by. Servers are uniquely identified by their address and VRF, so multiple servers can have the same address or host-name as long as the VRF is different. The default is the global VRF.
key	Set shared secret key with TACACS+ servers.
8	Specifies a string in a DES encrypted format instead of plain text. DES has been deprecated and should not be used. The default encryption format is now AES.
9	Specifies a string in an AES encrypted format instead of plain text. This is the default.
<i><key-string></i>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the tacacs-server key command. If no key value is specified, the global value is used.

Default No TACACS+ server is configured by default.

Mode Global Configuration

Usage A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable
- it cannot communicate with the switch properly due to the switch and the server having different secret keys

Examples To add the server tac1.company.com as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to 'secret' on the TACACS+ server 192.168.1.1, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server tac1.company.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

Examples (VRF-lite) To add the server tac1.company.com as the TACACS+ server host in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com vrf red
```

To remove the TACACS+ server 192.168.1.1 from the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host 192.168.1.1 vrf red
```

Related commands

- [aaa accounting commands](#)
- [aaa authentication login](#)
- [tacacs-server key](#)
- [tacacs-server timeout](#)
- [show tacacs+](#)

Command changes

- Version 5.5.4-0.1: DES encrypted format deprecated
- Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

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>

Syntax (VRF-lite) tcpdump [vrf <vrf-name>] <line>

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:
awplus# tcpdump ip

Example (VRF-lite) To start a tcpdump on interface vlan2 associated with a VRF instance red, enter the command:
awplus# tcpdump vrf red vlan2

Output

```
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.

telnet

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

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

Syntax (VRF-lite) telnet [vrf <vrf-name>] {<hostname>|[ip] <ipv4-addr>|[ipv6] <ipv6-addr>} [<port>]

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

Mode User Exec and Privileged Exec

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

```
awplus# telnet 10.2.2.2 2602
```

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

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

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

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

Example (VRF-lite) To open a telnet session to a remote host 192.168.0.1 associated with VRF instance red, use the command:

```
awplus# telnet vrf red ip 192.168.0.1
```

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>}`

Syntax (VRF-lite) `traceroute [vrf <vrf-name>] {<ip-addr>|<hostname>}`

Parameter	Description
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.
vrf	Apply the command to the specified VRF instance.
<vrf-name>	The name of the VRF instance.

Mode User Exec and Privileged Exec

Example `awplus# traceroute 10.10.0.5`

Example (VRF-lite) `awplus# traceroute vrf red 192.168.0.1`

Command changes Version 5.4.6-2.1: VRF-lite support added.

vrf

Overview Use this command to add a VRF name to a DHCP server's address pool. This enables the DHCP server to become VRF-aware and allocate IP addresses which are the same as other pools.

One of the benefits of using this command is that it allows you to share DHCP leases across multiple isolated networks.

Use the **no** variant of this command to remove a VRF name from the DHCP server pool.

Syntax vrf <vrf-name>
no vrf

Parameter	Description
<vrf-name>	The name of the specific VRF instance.

Default Global VRF

Mode DHCP Configuration

Usage notes You need to enter this **vrf** command before entering the **network (DHCP)** and **range** address commands.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

Example To add the VRF name 'red' to the DHCP pool named 'P1', use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P1
awplus(dhcp-config)# vrf red
```

To remove a VRF name from the DHCP pool named 'P1', use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P1
awplus(dhcp-config)# no vrf
```

Related commands [network \(DHCP\)](#)
[range](#)
[show ip dhcp pool](#)

Command changes Version 5.5.1-1.1: command added

Part 4: Access and Security

21 Traffic Control Commands

- Contents**
- **Introduction** on page 975
 - **class (htb)** on page 976
 - **class (priority)** on page 979
 - **class (wrr)** on page 981
 - **debug traffic-control** on page 983
 - **interface (traffic-control)** on page 984
 - **interface dynamic-virtual-bandwidth** on page 986
 - **l3-filtering enable** on page 988
 - **move rule (traffic-control)** on page 989
 - **policy (traffic-control)** on page 990
 - **red-curve** on page 992
 - **rule (traffic-control)** on page 994
 - **show debugging traffic-control** on page 996
 - **show running-config traffic-control** on page 997
 - **show traffic-control counters** on page 998
 - **show traffic-control interface** on page 1000
 - **show traffic-control policy** on page 1001
 - **show traffic-control red-curve** on page 1004
 - **show traffic-control rule config-check** on page 1006
 - **show traffic-control rule** on page 1007
 - **show traffic-control** on page 1008
 - **sub-class (htb)** on page 1009
 - **sub-class (priority)** on page 1011
 - **sub-class (wrr)** on page 1013
 - **sub-sub-class (htb)** on page 1015
 - **sub-sub-class (priority)** on page 1017
 - **sub-sub-class (wrr)** on page 1019
 - **traffic-control enable** on page 1021
 - **traffic-control** on page 1022

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure traffic control. For more information, see the [Traffic Control Feature Overview and Configuration Guide](#).

class (htb)

Overview Use this command to configure a hierarchy token bucket (HTB) class within a traffic control policy.

Use the **no** variant of this command to delete an existing class under a current policy.

Syntax

```
class <class-name> [cir <committed-rate>] [pir <peak-rate>]  
[bc <1-1000000000>] [be <1-1000000000>] [preference <0-7>] [queue-  
length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-  
name>]  
  
class <class-name> [cir <committed-rate>] [pir <peak-rate>]  
[bc <1-1000000000>] [be <1-1000000000>] [preference <0-7>] sub-  
class-policy htb  
  
no class <class-name>
```

Parameter	Description
<class-name>	Name of the class.
cir <committed-rate>	Set the Committed Information Rate (CIR) for the queue. This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional.
pir <peak-rate>	Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.
bc <1-1000000000>	Set the Committed Burst size (BC). This is the burst allowed above the CIR sent at the PIR rate.
be <1-1000000000>	Set the Excess Burst size (BE). This is the burst allowed above the PIR sent at the maximum rate.
preference <0-7>	Set the preference for a class to receive spare bandwidth. Preference for the class to receive spare bandwidth (highest is 7).
queue-length <2-65536>	Set the maximum queue length.
set-dscp <dscp-value>	Set the DSCP value to apply to the packets.
red-curve <red-curve-name>	Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied.
sub-class-policy	Specify that the class will contain sub-classes.
htb	Sub-classes will use the Hierarchy Token Bucket (HTB) queueing discipline.

Default BC and BE are assigned suitable values proportional to the CIR and PIR respectively, and are larger than the MTU. The PIR defaults to the CIR. The Preference defaults to 7 and the queue-length defaults to 1000 (if the class is a leaf). If the keyword <default> is used then the default RED curve is applied.

Mode Traffic-Control Policy for an HTB policy.

Usage If there is already a class in the same level that has the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

Examples To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit sub-
class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit sub-sub-class
policy htb
awplus(config-tc-subclass)#sub-sub-class ss01 cir 5mbit queue-
length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

Related **policy (traffic-control)**
commands **sub-class (htb)**
traffic-control

class (priority)

Overview Use this command to configure a priority queue class within a traffic control policy.

Use the **no** variant of this command to delete an existing priority class under a current policy.

Syntax `class <class-name> [priority-level <0-15>] [max <max-rate>]
[queue-length <2-65536>] [set-dscp <dscp-value>] [red-
curve <red-curve-name>]
class <class-name> [priority-level <0-15>] sub-class-policy
{priority|wrr|htb}
no class <class-name>`

Parameter	Description
<class-name>	Name of the class.
priority-level <0-15>	Set the priority level (15 is the highest). This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional.
max <max-rate>	Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).
queue-length <2-65536>	Set the maximum queue length in packets (only available on leaf queues when specifying sub-class policy).
set-dscp <dscp-value>	Set the DSCP value to apply to the packets (only available on leaf queues when specifying sub-class policy).
red-curve <red-curve-name>	Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied.
sub-class-policy	Create a sub-class within the policy.
priority	Sub-classes use the Priority Queue scheduling algorithm.
wrr	Sub-classes use the Weighted Round Robin scheduling algorithm.
htb	Sub-classes use the Hierarchy Token Bucket scheduling algorithm.

Default No priority class is applied. If the keyword <default> is used then the default RED curve is applied.

Mode Traffic Control Policy for a priority policy.

Usage If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

Examples To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5 sub-class-
policy priority
awplus(config-tc-class)#sub-class s01 priority-level 7 sub-sub-
class-policy priority
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
max 5mbit queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing policy class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

Related commands [policy \(traffic-control\)](#)
[sub-class \(htb\)](#)
[sub-class \(wrr\)](#)
[traffic-control](#)

class (wrr)

Overview Use this command to configure a Weighted Round-Robin (WRR) class within a traffic control policy.

Use the **no** variant of this command to delete an existing class under a current policy.

Syntax `class <class-name> [weight <1-100>] [queue-length <2-65536>]
[set-dscp <dscp-value>] [red-curve <red-curve-name>]
class <class-name> [weight <1-100>] sub-class-policy wrr
no class <class-name>`

Parameter	Description
<class-name>	Name of the class.
weight <1-100>	Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights. This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional.
queue-length <2-65536>	Set the maximum queue length in packets.
set-dscp <dscp-value>	Set the DSCP value to apply to packets.
red-curve <red-curve-name>	Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied.
sub-class-policy	Create a sub-class within the policy.
wrr	Sub-classes use the Weighted Round Robin queueing algorithm.

Default A weighted round-robin class has no DSCP value or sub-class policy. The queue length is 1000 by default. If the keyword <default> is used then the default RED curve is applied.

Mode Traffic-Control Policy for a WRR policy.

Usage If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

Examples To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30 sub-sub-class-
policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5 queue-
length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

Related commands [traffic-control](#)
[policy \(traffic-control\)](#)
[sub-class \(wrr\)](#)

debug traffic-control

Overview Use this command to enable traffic-control debugging. This will cause additional detailed debugging information to be logged and available using the show debugging traffic-control.

Use the **no** variant of this command to disable traffic-control debugging.

Syntax debug traffic-control
no debug traffic-control

Default Disabled

Mode Privileged Exec

Examples To enable traffic control debugging, use the commands:

```
awplus#debug traffic-control
```

To disable traffic control debugging, use the commands:

```
awplus#no debug traffic-control
```

Related commands [traffic-control](#)
[show debugging traffic-control](#)

interface (traffic-control)

Overview Use this command to configure interface specific parameters for traffic control.

Syntax `interface <interface-name> {overhead [<overhead-bytes>|ethernet]|virtual-bandwidth <bandwidth>|system-bandwidth <system-percentage>}`

Parameter	Description
<interface-name>	Name of interface to configure
overhead	Set overhead to add to each packet when calculating the packet size
<overhead-bytes>	Number of bytes to add to the packet for packet size calculations. The range is from 0 to 512 and the default is 0.
ethernet	Setting the overhead to 'ethernet' adds 24 bytes to the packet to account for preamble + CRC + inter-frame gap.
virtual-bandwidth	Specify the virtual-bandwidth of the interface. This is the maximum amount of traffic that traffic control will allow to be sent via the interface..
<bandwidth>	Value for the virtual bandwidth in kbit, mbit or gbits (for example, 5mbit).
system-bandwidth	Specify the percentage of the interface bandwidth to reserve for system traffic. The default when a traffic control policy is applied to the interface is 5%.
<system-percentage>	Percentage of the bandwidth to reserve for system traffic in the range from 1 to 99.

Default The default overhead is 0, the default bandwidth is the interface speed if it can be read. It is recommended to always set the virtual bandwidth when using traffic control. The system bandwidth default is 5%.

Mode Traffic-Control

Usage This command allows configuring traffic control parameters specific to the traffic egress interface.

Note that if you use Vista Manager EX's Auto Traffic Shaping feature, it will dynamically set the virtual bandwidth. In that situation, if you use this command to set the virtual bandwidth, your setting will only apply until Vista Manager EX dynamically overrides it. Your setting also won't be saved in the running config.

See the [interface dynamic-virtual-bandwidth](#) command for more information about the virtual bandwidth when using Auto Traffic Shaping.

Examples To rate limit eth1 to 10mbit while taking into account the ethernet framing overhead and reserving only 1% of the bandwidth for system traffic, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#interface eth1 overhead ethernet virtual-
bandwidth 10mbit system-bandwidth 1
```

Related commands [interface dynamic-virtual-bandwidth](#)
[show running-config traffic-control](#)
[show traffic-control interface](#)

Command changes Version 5.5.0-1.1: behavior changed when Auto Traffic Shaping is enabled in Vista Manager EX

interface dynamic-virtual-bandwidth

Overview Use this command to set or change the 'initial' virtual bandwidth value when Vista Manager EX has control of the virtual bandwidth on an interface. Vista Manager EX controls virtual bandwidth as part of Auto Traffic Shaping (ATS).

The device will use this command's virtual bandwidth in two situations:

- If you reboot the device, the device uses this virtual bandwidth until Vista Manager EX takes over control of the bandwidth
- It becomes the interface's virtual bandwidth if you turn off Auto Traffic Shaping in Vista Manager EX.

When Auto Traffic Shaping is on, the device does not store the interface's virtual-bandwidth in the device's running-config. This is to prevent Vista Manager EX's dynamic virtual bandwidth values from becoming permanent values.

Use the **no** variant of this command to indicate that Vista Manager EX no longer controls virtual bandwidth on this interface. Using the **no** variant does not change the current virtual-bandwidth value for the interface. If the current virtual-bandwidth value is not the default value, it will display in the device's running-config.

Syntax `interface <tunnel-name> dynamic-virtual-bandwidth controller <name> [initial-bandwidth <bandwidth>]`
`no interface <interface-name> dynamic-virtual-bandwidth`

Parameter	Description
<tunnel-name>	Name of the tunnel to configure
controller <name>	An identifier for the controller that is controlling the bandwidth. When Vista Manager EX is the controller, it will automatically set this value to 'vista-dynamic-management'. The name may contain alphanumeric, hyphen, underscore, comma, space or square brace characters, with a limit of 64 characters.
initial-bandwidth <bandwidth>	The value to apply as the interface's virtual-bandwidth when the interface starts up and if you turn ATS off. This value is the maximum amount of traffic that traffic control will allow the device to send via the interface (until the external manager changes it). Specify the value in kbit, mbit or gbits (for example, 5mbit).

Default If you turn on ATS in Vista Manager EX and do not use this command to set the initial bandwidth, then the device uses the virtual-bandwidth value from the command **interface (traffic-control)**.

Mode Traffic-Control

Examples To set an initial virtual-bandwidth of 10Mbps on tunnel2 when using Auto Traffic Shaping on Vista Manager EX, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#interface tunnel2 dynamic-virtual-bandwidth
controller vista-dynamic-management initial-bandwidth 10mbit
```

Related commands **traffic-control**
show running-config traffic-control
show traffic-control interface

Command changes Version 5.5.0-1.1: command added

l3-filtering enable

Overview Use this command to enable traffic control for bridged traffic on a bridge interface.

Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

Syntax l3-filtering enable
no l3-filtering enable

Default Traffic control is disabled by default for bridged traffic.

Mode Interface mode for a bridge interface

Example To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

Command changes Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

move rule (traffic-control)

Overview Use this command to change the identification of an existing traffic control rule.

Syntax move rule [<1-65535> to <1-65535>]

Parameter	Description
<1-65535>	Range of the rule ID to move from
<1-65535>	Range of the destination ID for the rule to move to

Default None

Mode Traffic-Control

Example To change rule ID 10 to rule ID 25, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#move rule 10 to 25
```

Related commands

- [rule \(traffic-control\)](#)
- [traffic-control](#)
- [show traffic-control](#)
- [show traffic-control rule](#)
- [show traffic-control rule config-check](#)

policy (traffic-control)

Overview Use this command to configure a traffic control policy, that can then be used with rules that have been created.

Use the **no** variant of this command to delete an existing policy.

Syntax `policy <policy-name> [priority|wrr|htb]`
`no policy <policy-name>`

Parameter	Description
<code><policy_name></code>	The name of the policy
<code>priority</code>	Use Priority Queueing (PQ)
<code>wrr</code>	Use Weighted Round Robin (WRR)
<code>htb</code>	Use Hierarchy Token Bucket (HTB)

Default No policies are configured

Mode Traffic-Control

Usage A policy specifies a top-level queueing discipline which determines the type of classes that can be configured under the policy. This command uses the Traffic-Control Policy mode.

Examples To configure a policy, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#
```

To delete an existing policy, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no policy p01 htb
```

Related commands

- class (htb)**
- class (priority)**
- class (wrr)**
- rule (traffic-control)**
- traffic-control**
- sub-class (htb)**
- sub-class (priority)**
- sub-class (wrr)**
- sub-sub-class (htb)**
- sub-sub-class (priority)**
- sub-sub-class (wrr)**

red-curve

Overview Use this command to allow configuration of a RED (Random Early Discard) curve template.

Use the **no** variant of this command to set the RED curve back to the default.

Syntax `red-curve <red-curve-name> [limit <4-127>] [avpkt <64-1518>]
[min <3-126>] [max <4-127>] [probability <1-100>]
[ecn [ecn-drop]]
no red-curve [<red-curve-name>]`

Parameter	Description
<code><red-curve-name></code>	The RED curve name.
<code>limit <4-127></code>	The hard queue length limit (in packets) for the RED curve. Once the queue length reaches the limit, all packets are dropped.
<code>avpkt <64-1518></code>	The average packet size to use for queue size calculations in bytes.
<code>min <3-126></code>	The minimum queue length for random early discard (in packets). Between <min> and <max> the drop probability will increase linearly.
<code>max <4-127></code>	The maximum queue length where packets are probabilistically dropped. At <max> the drop probability equals <probability>. Beyond <max> the drop or marking probability is 100%.
<code>probability <1-100></code>	The probability of a packet being dropped when queue-length reaches <max>. The drop probability increases linearly from 0 to <probability> in between <min> and <max>.
<code>ecn</code>	Use explicit congestion notification marking instead of dropping the packet.
<code>ecn-drop</code>	When average queue size exceeds <max> drop packets instead of marking.

Default The default RED curve is `red-curve default limit 127 avpkt 576B min 10 max 32 prob 2`.

Mode Traffic-control

Usage notes The RED curve template can later be applied to a traffic control class, sub-class, or sub-sub-class.

Example To configure a RED curve with ECN dropping and the default curve shape, use the commands:

```
awplus# configure terminal
awplus(config)# traffic-control
awplus(config-tc)# red-curve red-ecn ecn
```

To configure an aggressive RED curve, use the commands:

```
awplus# configure terminal
awplus(config)# traffic-control
awplus(config-tc)# red-curve aggressive min 5 max 50 probability
70
```

Related commands

- class (htb)**
- class (priority)**
- class (wrr)**
- show traffic-control policy**
- show running-config traffic-control**
- show traffic-control red-curve**
- sub-class (htb)**
- sub-class (priority)**
- sub-class (wrr)**
- sub-sub-class (htb)**
- sub-sub-class (priority)**
- sub-sub-class (wrr)**

rule (traffic-control)

Overview Use this command to create a traffic-control rule.

Use the **no** variant of this command to remove a traffic-control rule

Syntax rule [<1-65535>] match <application> from <source-entity> to
<destination-entity> policy <policy>
no rule [<1-65535>]

Parameter	Description
<1-65535>	The rule ID is an integer in the range from 1 to 65535. If you do not designate a rule ID, one will be automatically generated and it will be greater than the current highest rule ID. Lower IDs have higher priority.
match	Application traffic to match
<application>	Application name. You can use the tab key to auto-complete application names.
from	Set the source of the entity
<source_entity>	Source entity name. Entities represent logical grouping of subnets, hosts or interfaces. You can use the tab key to auto-complete entity names.
to	Set the destination of the entity
<destination_entity>	Source entity name. Entities represent logical grouping of subnets, hosts or interfaces.
policy	Policy to apply to matched traffic
<policy>	Traffic control policy. This consists of a top-level policy name followed by the name of a class within that policy, and sub-class (of the class) and a sub-sub-class if applicable. Examples are: p01.c03 p01.c03.sc02 p01.c03.scc02.ssc01 In these examples, p01 is the policy name, c03 is the class name, sc02 is the sub-class, and ssc01 is the sub-sub-class.

Default No rules

Mode Traffic-Control

Usage Rules are used to apply traffic-control policies to a type of traffic. When traffic control is enabled and no rules are added, a default traffic-control policy is installed on all supported interfaces.

If the application, source entity or destination entity specified in the rule is not configured correctly, the rule is not valid and is not installed.

You can change the rule order by using the move rule (traffic-control) command.

Rules are applied to destination interfaces in the order of their ID (lower IDs are applied first). If traffic matches a rule, then the rest are ignored. If traffic does not match any rule, then it is classified to the default class.

A rule can specify the system class as the policy. System traffic is high priority traffic that is allocated a fixed amount of bandwidth on an interface. Use the interface (traffic-control) command to configure system bandwidth on an interface.

Examples To configure a rule, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#rule 10 match ftp from wan to private policy
p01.c02.sc03
```

To delete a rule, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no rule 10
```

Related commands

- interface (traffic-control)**
- move rule (traffic-control)**
- policy (traffic-control)**
- traffic-control**
- show running-config traffic-control**
- show traffic-control rule**

show debugging traffic-control

Overview Use this command to display the status of traffic control debugging

Syntax show debugging traffic-control

Mode Privileged Exec

Example To show if traffic-control debugging is on or off, run the command:

```
awplus#show debugging traffic-control
```

Output The following shows typical output.

Example output from show debugging traffic-control

```
awplus#show debugging traffic-control  
Traffic-control Debugging Status: off
```

Related commands [debug traffic-control](#)
[show debugging](#)

show running-config traffic-control

Overview Use this command to display the current traffic control configuration.

Note that Vista Manager EX will dynamically set the virtual bandwidth if you use its Auto Traffic Shaping feature. In that situation, this command will display the **interface dynamic-virtual-bandwidth** command instead of any virtual bandwidth added with the **interface (traffic-control)** command.

Syntax show running-config traffic-control

Mode Privileged Exec

Example To show the traffic control configuration section of the running configuration, use the command:

```
awplus#show running-config traffic-control
```

Output The following shows typical output.

Example output from show running-config traffic-control

```
awplus#show running-config traffic-control
traffic-control
policy p1 priority
class c1 priority-level 15
rule 10 match selfmade1 from lan to inet policy p1.c1
traffic-control enable
!
```

Related commands

- interface (traffic-control)**
- show running-config**
- show traffic-control counters**
- show traffic-control interface**
- show traffic-control policy**
- show traffic-control rule**
- show traffic-control rule config-check**
- traffic-control**

Command changes Version 5.5.0-1.1: behavior changed when Auto Traffic Shaping is enabled in Vista Manager EX

show traffic-control counters

Overview Use this command to display counters related to traffic control. This command displays counters for the number of packets sent, queued or dropped by each traffic control class. The information is shown by each interface. There is an overall counter for the policy, and counters for each leaf class in the policy.

If no interface name is specified then information for all interfaces with traffic control policies applied is displayed.

Syntax show traffic-control counters [<interface-name>]

Parameter	Description
<i><interface-name></i>	Name of Interface to display traffic control counters

Mode Privileged Exec

Examples To show the traffic control counters for all interfaces, use the commands:
awplus#show traffic-control counters

Example output from show traffic-control counters

```
awplus#show traffic-control counters
Traffic Control Counters
Interface eth1:
```

Class	Counter	Bytes	Packets
A	Sent	0	
0	Currently Queued	0	0
	Dropped		0
A.B5001	Sent	0	0
	Currently Queued	0	0
	Dropped		0
A.B5002	Sent	0	0
	Currently Queued	0	0
	Dropped		0
A.default	Sent	0	0
	Currently Queued	0	0
	Dropped		0
system	Sent	0	0
	Currently Queued	0	0
	Dropped		0

```
Interface eth2:
```

Class	Counter	Bytes	Packets
A	Sent	58681224	232862
	Currently Queued	0	383
	Dropped		1039845
A.B5001	Sent	10671444	42347
	Currently Queued	32004	128
	Dropped		164954
A.B5002	Sent	17661924	70087
	Currently Queued	32004	127
	Dropped		123470
A.default	Sent	30348360	120430
	Currently Queued	32004	128
	Dropped		751421
system	Sent	42	1
	Currently Queued	0	0
	Dropped		0

Related [show running-config traffic-control commands](#)

show traffic-control interface

Overview Use this command to display information about interfaces known to traffic control, such as the applied policy, the virtual-bandwidth configured on the interface, the bandwidth reserved for system traffic and the overhead applied to the packet size calculations. If no interface name is specified, information is shown for all interfaces known to traffic control.

Syntax show traffic-control interface [<interface-name>]

Parameter	Description
<interface-name>	Name of interface to display information

Mode Privileged Exec

Examples To show traffic control information for all interfaces, use the command:
awplus#show traffic-control interface

Output The following shows typical output.

Example output from show traffic-control interface

```
awplus#show traffic-control interface
Traffic Control Interface Information

eth1:
Policy:                A
Virtual bandwidth:     Not set (optional)
System bandwidth:      5%
Packet overhead:       0 Bytes

eth2:
Policy:                A
Virtual bandwidth:     2000 kbit
System bandwidth:      5%
Packet overhead        24 Bytes (Ethernet transport layer)
```

Related commands [interface \(traffic-control\)](#)
[show running-config traffic-control](#)

show traffic-control policy

Overview Use this command to show information about the configured traffic control policies and classes. This command shows the configured traffic control policies and the interfaces that they are applied to. Only non-default configuration parameters are shown.

If no policy name is given, all configured policies are displayed.

Syntax show traffic-control policy [*<policy-name>*]

Parameter	Description
<i><policy-name></i>	Name of policy to display

Mode Privileged Exec

Examples To show all traffic control policies, use the command:

```
awplus#show traffic-control policy
```

To show a specific traffic control policy, use the command:

```
awplus#show traffic-control policy A
```

Output The following shows typical output.

Example output from show traffic-control policy

```
awplus#show traffic-control policy
Traffic Control Policies:
Policy A:
  Type: wrr
  Applied interfaces: eth1 eth2
  Classes:
    Class B5001:
      Weight: 30
    Class B5002:
      Weight: 60
      Red curve: default
Policy P:
  Type: priority
  Applied interfaces: None
  Classes:
    Class P10:
      Priority: 10
      Peak rate (PIR): 5000kbit
    Class P3:
      Priority: 3
      Peak rate (PIR): 8000kbit
      Sub-queue type: htb
      Red curve: TCP_session_1
    Class H:
      Committed rate (CIR): 3000kbit
      Burst (Bc): 100000B
    Class I:
      Committed rate (CIR): 5000kbit
      Burst (Bc): 100000B
    Class P2:
      Priority: 2
      Red curve: TCP_session_2
Policy token-bucket:
  Type: htb
  Applied interfaces: None
  Classes:
    Class A:
      Committed rate (CIR): 5000kbit
      Peak rate (PIR): 6000kbit
      Preference: 2
    Class B:
      Committed rate (CIR): 2000kbit
      Peak rate (PIR): 4000kbit
      Burst (Bc): 100000B
      Excess Burst (Be): 100000B
      Preference: 3
      Sub-queue type: htb
    Class C:
      Committed rate (CIR): 2000kbit
      Peak rate (PIR): 4000kbit
      Burst (BC): 50000B
    Class D:
      Committed rate (CIR): 1000kbit
      Peak rate (PIR): 4000kbit
      Burst (Bc): 50000B
      Sub-queue type: htb
    Class E:
      Committed rate (CIR): 500kbit
      Peak rate (PIR): 4000kbit
      Burst (Bc): 50000B
      Set DSCP: af23
    Class F:
```

Committed rate (CIR):	500kbit
Peak rate (PIR):	4000kbit
Burst (Bc):	50000B
Set DSCP:	af31

Related **show running-config**
commands **show running-config traffic-control**

show traffic-control red-curve

Overview Use this command to show configured RED curve templates.

Syntax `show traffic-control red-curve <red-curve-name>`

Parameter	Description
<code><red-curve-name></code>	The name of the RED curve. The default RED curve is red-curve default limit 127 avpkt 576B min 10 max 32 prob 2.

Mode Privileged Exec

Usage notes If you have not configured some parameters, default values will display. If no RED curve name is given, all configured RED curves are shown.

Example To show all RED curves, use the command:

```
awplus# show traffic-control red-curve
```

To show a specified red curve called "TCP_session_1", use the command:

```
awplus# show traffic-control red-curve TCP_session_1
```


Output The following shows typical output.

Example output from show traffic-control red-curve

```
awplus#show traffic-control red-curve
Traffic Control RED Curves:

RED curve default:
  Average packet size: 576 bytes
  Minimum: 10 packets
  Maximum: 32 packets
  Limit: 127 packets
  Drop probability: 2%
  ECN marking: disabled

RED curve TCP_session_1:
  Average packet size: 576 bytes
  Minimum: 20 packets
  Maximum: 60 packets
  Limit: 127 packets
  Drop probability: 20%
  ECN marking: disabled
```

Example output from show traffic-control red-curve TCP_session_1

```
awplus#show traffic-control red-curve TCP_session_1
Traffic Control RED Curves
RED curve TCP_session_1:
  Average packet size: 576 bytes
  Minimum: 20 packets
  Maximum: 60 packets
  Limit: 127 packets
  Drop probability: 20%
  ECN marking: disabled
```

Related commands

- [red-curve](#)
- [show running-config](#)
- [show running-config traffic-control](#)
- [show traffic-control policy](#)

show traffic-control rule config-check

Overview Use this command to show information about traffic control rule validity.

Syntax show traffic-control rule config-check

Mode Privileged Exec

Usage An asterisk is printed before each rule that is invalid. To help determine why the rule is invalid, the show traffic-control rule config-check command will print the reasons why the rule is invalid. Information is only shown for invalid rules. If all rules are valid, a message will be printed showing all rules are valid.

Example To check if configured rules are valid, use the commands:

```
awplus#show traffic-control rule config-check
```

Output The following shows typical output.

Example output from show traffic-control rule config-check

```
awplus#show traffic-control rule config-check

Rule 30:
  "From" entity does not exist
  "To" entity does not exist
  Policy doesn't exist or is not leaf
```

Related commands

- [move rule \(traffic-control\)](#)
- [rule \(traffic-control\)](#)
- [show traffic-control rule](#)
- [show running-config traffic-control](#)

show traffic-control rule

Overview Use this command to show specific rules or a complete list of rules configured for traffic control.

Syntax show traffic-control rule [<1-65535>]

Parameter	Description
<1-65535>	The ID of the rule you want to display. If no ID is entered, all rules are displayed.

Mode Privileged Exec

Usage An asterisk will be printed at the start of a row if the rule is invalid. The rules are shown in a table showing the rule ID, the application, source and destination that the rule matches on and the policy and class that the matching traffic will be sent to.

Examples To show a list of all traffic control rules configured, use the command:

```
awplus#show traffic-control rule
```

To show traffic control rule 10 configured, use the command:

```
awplus#show traffic-control rule 10
```

Output The following shows typical output.

Example output from show traffic-control rule

```
awplus#show traffic-control rule
[* - Rule is not valid - see "show traffic-control rule config-check"]
  ID      APP      From      To      Policy
-----
  10      udp-5001      ipv6.eth1      ipv6.eth2      A.B5001
  20      udp-5002      ipv6.eth1      ipv6.eth2      A.B5002
* 30      aserf        asdf        fasdf        sadf.asdf
```

Related commands

- [move rule \(traffic-control\)](#)
- [rule \(traffic-control\)](#)
- [show running-config traffic-control](#)
- [show traffic-control](#)
- [show traffic-control rule config-check](#)

show traffic-control

Overview Use this command to display a brief overview of the status of the traffic control information on the router.

Syntax show traffic-control

Mode Privileged Exec

Usage This command shows if traffic control is enabled, how many rules are configured and how many interfaces have a virtual bandwidth applied.

Example To show an overview of the status of the traffic control information, use the commands:

```
awplus# show traffic-control
```

Output The following shows typical output.

Example output from show traffic-control

```
awplus#show traffic-control
Traffic control is enabled
Policy configured on 5 interfaces
2 rules configured (2 valid rules)
Virtual-bandwidth configured on 1 interfaces
```

Related commands [traffic-control](#)
[traffic-control enable](#)

sub-class (htb)

Overview Use this command to configure a hierarchy token bucket (HTB) sub-class within an existing class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

Syntax `sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>] [bc <1-1000000000>] [be <1-1000000000>] [preference <0-7>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`
`sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>] [bc <1-1000000000>] [be <1-1000000000>] [preference <0-7>] sub-sub-class-policy htb`
`no sub-class <class-name>`

Parameter	Description
<code><class-name></code>	Name of the class.
<code>cir <committed-rate></code>	Set the Committed Information Rate (CIR) for the queue. Specified in kbit/mbit/gbit per second, 1kbit-100gbit. This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional.
<code>pir <peak-rate></code>	Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.
<code>bc <1-1000000000></code>	Set the Committed Burst size (BC). This is the burst allowed above the CIR, sent at the PIR rate.
<code>be <1-1000000000></code>	Set the Excess Burst size (BE). This is the burst allowed above the PIR, sent at the maximum rate.
<code>preference <0-7></code>	Set the preference for a class to receive spare bandwidth (highest is 7).
<code>queue-length <2-65536></code>	Set the maximum queue length in packets.
<code>set-dscp <dscp-value></code>	Set the DSCP value to apply to the packets.
<code>red-curve <red-curve-name></code>	Apply a random early discard template with the sub-class and enter the name of the red curve template to apply.
<code>sub-sub-class-policy</code>	Specify that the sub-class will contain sub-sub-classes.
<code>htb</code>	Sub-sub-classes will use the Hierarchy Token Bucket (HTB) queueing discipline.

Default BC and BE are assigned suitable values proportional to the CIR and PIR respectively and are larger than the MTU. PIR defaults to the CIR. Preference defaults to 7 and the queue length default to 1000 if the class is a leaf.

Mode Traffic-Control Class for an HTB sub-class policy.

Usage If there is already a sub-class in the same level with the specified name, the command will replace the configuration of the existing sub class if it does not have any sub-sub-classes.

If you specify a sub-sub-class policy, this command puts you into sub-class mode so you can specify the sub-sub-class.

Examples To configure a leaf sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit sub-
class-policy htb
wplus(config-tc-class)#sub-class s02 cir 20mbit queue-length 200
red-curve s02-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

Related commands

- class (htb)**
- class (priority)**
- policy (traffic-control)**
- sub-sub-class (htb)**
- traffic-control**

sub-class (priority)

Overview Use this command to configure a priority queue sub-class within a class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

Syntax sub-class <class-name> [priority-level <0-15>] [max <max-rate>] [queue-length <2-65536>] [set-dscp <dscp_value>] [red-curve <red-curve-name>]
sub-class <class-name> [priority-level <0-15>] sub-sub-class-policy {priority|wrr|htb}
no sub-class <class-name>

Parameter	Description
<class-name>	Name of the class.
priority-level <0-15>	Set the priority level (15 is the highest). This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional.
max <max-rate>	Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).
queue-length <2-65536>	Set the maximum queue length in packets.
set-dscp<dscp_value>	Set the DSCP value to apply to the packets.
red-curve <red-curve-name>	Apply a random early discard template with the sub class and enter the name of the red curve template to apply.
sub-sub-class-policy	Create a sub-sub-class for the policy.
priority	Sub-sub-classes will use the Priority Queue queueing algorithm.
wrr	Sub-sub-classes will use the Weighted Round Robin (WRR) queueing algorithm.
htb	Sub-classes will use the Hierarchy Token Bucket (HTB) queueing algorithm.

Default A priority queue sub class has no max rate, DSCP value or sub-sub class policy. The queue length is 1000 by default if the class is a leaf.

Mode Traffic-Control Class for a priority sub-class policy.

Usage If there is already a sub-class in the same level with the specified name, the command will replace the configuration of the existing sub class if it does not have any sub-sub classes.

If a sub-sub class policy is specified, this command uses the Traffic-Control Class mode to apply it.

Examples To configure a sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5 sub-class-policy priority
awplus(config-tc-class)#sub-class s02 priority-level 8 max
50mbit queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

Related commands

- class (priority)**
- policy (traffic-control)**
- sub-sub-class (htb)**
- sub-sub-class (priority)**
- sub-sub-class (wrr)**
- traffic-control**

sub-class (wrr)

Overview Use this command to configure a Weighted Round-Robin (WRR) sub-class within a class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

Syntax sub-class <class-name> [weight <1-100>] [queue-length <2-65536>]
[set-dscp <dscp-value>] [red-curve <red-curve-name>]
sub-class <class-name> [weight <1-100>] sub-sub-class-policy wrr
no sub-class <class-name>

Parameter	Description
<class-name>	Name of the sub-class.
weight<1-100>	Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights. This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional.
queue-length<2-65536>	Set the maximum queue length in packets.
set-dscp	Set the DSCP value to apply to packets.
<dscp-value>	DSCP value as an integer or lower-case DSCP name.
red curve <red-curve-name>	Apply a random early discard template with the sub-class and enter the name of the red curve template to apply.
sub-sub-class-policy	Create a sub-sub-class within the policy.
wrr	Sub sub classes use the Weighted Round Robin queueing discipline.

Default A weighted round-robin sub class has no DSCP value or sub-sub-class policy. The queue length is 1000 by default.

Mode Traffic-Control Class for a WRR sub-class policy.

Usage If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub class policy is specified, this command uses the Traffic-Control Class mode to apply it.

Examples To configure a sub-class as a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c02 weight 30 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s02 weight 40 queue-length 200
red-curve s02-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

Related commands

- class (priority)**
- class (wrr)**
- policy (traffic-control)**
- traffic-control**
- sub-sub-class (wrr)**

sub-sub-class (htb)

Overview Use this command to configure a Hierarchy Token Bucket (HTB) sub-sub-class for a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

Syntax `sub-sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>] [bc <1-1000000000>] [be <1-1000000000>] [preference <0-7>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`
`no sub-sub-class <class-name>`

Parameter	Description
<class-name>	Name of the sub-sub-class.
cir <committed-rate>	Set the Committed Information Rate (CIR) for the queue. Specified in kbit/mbit/gbit per second, 1kbit-100gbit. This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional.
pir <peak-rate>	Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.
bc <1-1000000000>	Set the Committed Burst size (BC). This is the burst allowed above the CIR, sent at the PIR rate.
be <1-1000000000>	Set the Excess Burst size (BE). This is the burst allowed above the PIR, sent at the maximum rate..
preference <0-7>	Set the preference for a class to receive spare bandwidth (highest is 7).
queue-length <2-65536>	Set the maximum queue length.
set-dscp <dscp-value>	Set the DSCP value to apply to the packets.
red-curve <red-curve-name>	Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.

Default BC and BE are assigned suitable values proportional to the CIR and PIR respectively and are larger than the MTU. PIR defaults to the CIR. Preference defaults to 7 and Queue length defaults to 1000.

Mode Traffic-Control Sub-class for an HTB sub-sub-class policy.

Usage If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

Examples To configure a sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit sub-
class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit
```

To configure a leaf sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit sub-
class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit sub-sub-class-
policy htb
awplus(config-tc-subclass)#sub-sub-class ss01 cir 5mbit queue-
length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

Related commands

- policy (traffic-control)**
- sub-class (htb)**
- sub-class (priority)**
- traffic-control**

sub-sub-class (priority)

Overview Use this command to configure a priority queue sub-sub-class for a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

Syntax `sub-sub-class <class-name> [priority-level <0-15>] [max <max-rate>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`
`no sub-sub-class <class-name>`

Parameter	Description
<code><class-name></code>	Name of the class.
<code>priority-level <0-15></code>	Set the priority level (15 is the highest). This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional.
<code>max <max-rate></code>	Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).
<code>queue-length <2-65536></code>	Set the maximum queue length in packets.
<code>set-dscp <dscp-value></code>	Set the DSCP value to apply to the packets.
<code>red-curve <red-curve-name></code>	Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.

Default A priority queue sub-sub-class has no max rate or DSCP value. The queue length is 1000.

Mode Traffic-Control Sub-class for a priority sub-sub-class policy.

Usage If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

Examples To configure a sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
awplus(config-tc-class)#sub-class s01 priority-level 7
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
```

To configure a sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5 sub-class-
policy priority
awplus(config-tc-class)#sub-class s01 priority-level 7 sub-sub-
class-policy priority
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
max 5mbit queue-length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

Related commands [traffic-control](#)
[policy \(traffic-control\)](#)
[sub-class \(priority\)](#)

sub-sub-class (wrr)

Overview Use this command to configure a Weighted Round-Robin (WRR) sub-sub-class within a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

Syntax `sub-sub-class <class-name> [weight <1-100>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`
`no sub-sub-class <class-name>`

Parameter	Description
<code><class-name></code>	Name of the sub-class.
<code>weight <1-100></code>	Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights. This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional.
<code>queue-length <2-65536></code>	Set the maximum queue length in packets.
<code>set-dscp <dscp-value></code>	Set the DSCP value to apply to packets.
<code>red-curve <red-curve-name></code>	Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.

Default A weighted round-robin sub-sub-class has no DSCP value. The queue length is 1000 by default.

Mode Traffic-Control Sub-class for a WRR sub-sub-class policy.

Usage If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

Examples To configure a sub-sub-class as a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30 sub-sub-class
policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5 queue-
length 200
```

To configure a sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30 sub-sub-class-
policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5 queue-
length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

Related commands

- traffic-control**
- policy (traffic-control)**
- sub-class (priority)**
- sub-class (wrr)**

traffic-control enable

Overview Use this command to enable traffic control.

Use the **no** variant of this command to disable traffic control without losing your existing traffic control configuration.

Syntax traffic-control enable
no traffic-control enable

Default Disabled

Mode Traffic-Control

Usage When traffic control is enabled and no rules are added, a default queueing discipline is applied to all interfaces that support traffic control. You can use the policy command to configure traffic control policies and the rule (traffic-control) command to apply the configured policies to the traffic.

Examples To enable traffic control, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#traffic-control enable
```

To disable traffic control, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no traffic-control enable
```

Related commands **policy (traffic-control)**
rule (traffic-control)
traffic-control

traffic-control

Overview Use this command to enter into Traffic-Control configuration mode.

Use the **no** variant of this command to remove all traffic control configuration.

Syntax traffic-control
no traffic-control

Default Disabled

Mode Global Configuration

Usage This command enters you into Traffic-Control configuration mode.

In Traffic-Control Configuration mode you can:

- enable or disable traffic control
- create and delete traffic control policies
- create, move and delete rules for traffic control
- set and unset packet overhead, system bandwidth and virtual bandwidth of interfaces

Examples To configure traffic-control, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#
```

To remove all traffic control configuration, use the commands:

```
awplus#configure terminal
awplus(config)#no traffic-control
awplus(config)#
```

Related commands

- class (htb)**
- class (priority)**
- class (wrr)**
- debug traffic-control**
- interface (traffic-control)**
- move rule (traffic-control)**
- policy (traffic-control)**
- rule (traffic-control)**
- traffic-control**
- show debugging traffic-control**
- show running-config traffic-control**
- show traffic-control**
- show traffic-control counters**
- show traffic-control interface**
- show traffic-control policy**
- show traffic-control rule**
- show traffic-control rule config-check**
- sub-class (htb)**
- sub-class (priority)**
- sub-class (wrr)**
- sub-sub-class (htb)**
- sub-sub-class (priority)**
- sub-sub-class (wrr)**

22

AAA Commands

- Contents**
- **Introduction** on page 1025
 - **aaa accounting commands** on page 1026
 - **aaa accounting login** on page 1028
 - **aaa accounting openvpn** on page 1031
 - **aaa accounting update** on page 1033
 - **aaa authentication 2fa-registration default group** on page 1035
 - **aaa authentication download-portal** on page 1037
 - **aaa authentication enable default group tacacs+** on page 1039
 - **aaa authentication enable default local** on page 1042
 - **aaa authentication isakmp** on page 1043
 - **aaa authentication login** on page 1044
 - **aaa authentication openvpn** on page 1047
 - **aaa authorization commands** on page 1050
 - **aaa authorization config-commands** on page 1052
 - **aaa group server** on page 1053
 - **aaa local authentication attempts lockout-time** on page 1055
 - **aaa local authentication attempts max-fail** on page 1056
 - **aaa local authentication attempts max-fail remote-login-only** on page 1058
 - **aaa login fail-delay** on page 1059
 - **accounting login** on page 1060
 - **authorization commands** on page 1061
 - **clear aaa local user lockout** on page 1063
 - **debug aaa** on page 1064
 - **login authentication** on page 1065
 - **proxy-port** on page 1066
 - **radius-secure-proxy aaa** on page 1067
 - **server (radsecproxy-aaa)** on page 1068
 - **server mutual-authentication** on page 1070
 - **server name-check** on page 1071
 - **server trustpoint** on page 1072
 - **show aaa local user locked** on page 1074
 - **show aaa server group** on page 1076
 - **show debugging aaa** on page 1077
 - **show radius server group** on page 1078
 - **undebug aaa** on page 1080

Introduction

Overview AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These functions can be applied in a variety of methods with a variety of servers.

The purpose of the AAA commands is to map instances of the AAA functions to sets of servers. The Authentication function can be performed in multiple contexts, such as authentication of users logging in at a console, or 802.1X-Authentication of devices connecting to Ethernet ports.

For each of these contexts, you may want to use different sets of servers for examining the proffered authentication credentials and deciding if they are valid. AAA Authentication commands enable you to specify which servers will be used for different types of authentication.

This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the [**AAA and Port_Authentication Feature Overview and Configuration Guide**](#).

aaa accounting commands

Overview This command configures and enables TACACS+ accounting on commands entered at a specified privilege level. Once enabled for a privilege level, accounting messages for commands entered at that privilege level will be sent to a TACACS+ server.

In order to account for all commands entered on a device, configure command accounting for each privilege level separately.

The command accounting message includes, the command as entered, the date and time the command finished executing, and the user-name of the user who executed the command.

Use the **no** variant of this command to disable command accounting for a specified privilege level.

Syntax `aaa accounting commands <1-15> default stop-only group tacacs+
no aaa accounting commands <1-15> default`

Parameter	Description
<1-15>	The privilege level being configured, in the range 1 to 15.
default	Use the default method list, this means the command is applied globally to all user exec sessions.
stop-only	Send accounting message when the commands have stopped executing.
group	Specify the server group where accounting messages are sent. Only the tacacs+ group is available for this command.
tacacs+	Use all TACACS+ servers configured by the tacacs-server host command.

Default TACACS+ command accounting is disabled by default.

Mode Global Configuration

Usage notes This command only supports a **default** method list, this means that it is applied to every console and VTY line.

The **stop-only** parameter indicates that the command accounting messages are sent to the TACACS+ server when the commands have stopped executing.

The **group tacacs+** parameters signifies that the command accounting messages are sent to the TACACS+ servers configured by the **tacacs-server host** command.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured with only the first reachable server being used. If no server is found, the accounting message is dropped.

Command accounting cannot coexist with triggers. An error message is displayed if you attempt to enable command accounting while a trigger is configured. Likewise, an error message is displayed if you attempt to configure a trigger while command accounting is configured.

Examples To configure command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 1 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 7 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 1 default
awplus(config)# no aaa accounting commands 7 default
awplus(config)# no aaa accounting commands 15 default
```

Related commands [aaa authentication login](#)
[aaa accounting login](#)
[accounting login](#)
[tacacs-server host](#)

aaa accounting login

Overview This command configures RADIUS and TACACS+ accounting for login shell sessions. The specified method list name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, then this creates a default method list that is applied to every console and VTY line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to remove an accounting method list for login shell sessions configured by an **aaa accounting login** command. If the method list being deleted is already applied to a console or VTY line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

Syntax `aaa accounting login {default|<list-name>}{start-stop|stop-only|none} {group {radius|tacacs+|<group-name>}}`
`no aaa accounting login {default|<list-name>}`

Parameter	Description
default	Default accounting method list.
<list-name>	Named accounting method list.
start-stop	Start and stop records to be sent.
stop-only	Stop records to be sent.
none	No accounting record to be sent.
group	Specify the servers or server group where accounting packets are sent.
radius	Use all RADIUS servers configured by the radius-server host .
tacacs+	Use all TACACS+ servers configured by the tacacs-server host command.
<group-name>	Use the specified RADIUS server group, as configured by the aaa group server command.

Default Accounting for login shell sessions is disabled by default.

Mode Global Configuration

Usage notes This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name **default** and any number of other named method lists. The name of any method list that you define can then be used as the *<list-name>* parameter in the **accounting login** command.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <group-name>** : use the specified RADIUS server group configured with the **aaa group server** command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+** : use all TACACS+ servers configured by **tacacs-server host** command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting login default
```

Related commands

- aaa accounting commands**
- aaa authentication login**
- aaa accounting login**
- accounting login**
- radius-server host**
- tacacs-server host**

aaa accounting openvpn

Overview Use this command to configure the default accounting method list for OpenVPN tunnels. The default accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. The default accounting method list is automatically applied to OpenVPN tunnels.

Use the **no** variant of this command to disable AAA accounting for OpenVPN tunnels globally.

Syntax `aaa accounting openvpn default {start-stop|stop-only|none} group {<group-name>|radius}`
`no aaa accounting openvpn default`

Parameter	Description
default	Configure the default accounting method list
start-stop	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
stop-only	Only sends a stop accounting message at the end of the session.
none	No accounting record sent.
group	Use a server group
<group-name>	Server group name.
radius	Use all RADIUS servers.

Default RADIUS accounting for OpenVPN tunnels is disabled by default (there is no default server set by default).

Mode Global Configuration

Usage notes This command configures the default accounting method list which is automatically applied to all OpenVPN tunnels.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius**: use all RADIUS servers configured by **radius-server host** command.
- **group <group-name>**: use the specified RADIUS server group configured with the **aaa group server** command.

Examples To enable RADIUS accounting for OpenVPN tunnels, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting openvpn default start-stop group
radius
```

To disable RADIUS accounting for OpenVPN tunnels, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting openvpn default
```

Related commands

- aaa accounting update**
- aaa authentication openvpn**
- aaa group server**
- radius-server host**
- show aaa server group**
- tunnel mode openvpn tap**
- tunnel mode openvpn tun**

Command changes Version 5.5.4-2.3: command added

aaa accounting update

Overview This command enables periodic accounting reporting to the RADIUS accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

Syntax aaa accounting update [periodic <1-65535>]
no aaa accounting update

Parameter	Description
periodic	Send accounting records periodically.
<1-65535>	The interval to send accounting updates (in minutes). The default is 30 minutes.

Default Disabled

Mode Global Configuration

Usage notes Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting reporting is enabled, interim accounting records are sent at the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is re-enabled, unless this interval is specified.

Examples To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting updates wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting update
```

Related commands [radius-server host](#)

aaa authentication 2fa-registration default group

Overview Use this command to set authentication methods for Two-Factor Authentication (2FA) user self-registration.

Use the **no** variant of this command to unset authentication methods for 2FA user self-registration.

```
Syntax aaa authentication 2fa-registration default group {ldap|radius|
<group-name>}
no aaa authentication 2fa-registration default
```

Parameter	Description
ldap	Use all LDAP servers configured by the ldap-server name command.
radius	Use all RADIUS servers configured by the radius-server host command.
<group-name>	The name of the LDAP or RADIUS server group to authenticate self-registration users with.

Default No servers are configured by default

Mode Global Configuration

Examples To configure LDAP servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group ldap
```

To configure RADIUS servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group radius
```

To configure a selected LDAP or RADIUS group of servers called 'GRP1' to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group GRP1
```

To remove the configured server group for 2FA self-registration to authenticate with, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication 2fa-registration default
```

Related commands [2fa self-registration port service 2fa](#)

Command changes Version 5.5.3-0.1: command added

aaa authentication download-portal

Overview Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

Syntax `aaa authentication download-portal default group [<group-name>|radius|ldap]`
`no aaa authentication download-portal default`

Parameter	Description
<code><group-name></code>	Server group name.
<code>radius</code>	Use all RADIUS servers
<code>ldap</code>	Use all LDAP servers

Default Authentication for Download Portal clients is disabled by default.

Mode Global Configuration

Usage notes There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the **radius-server host** command.
- **group ldap:** use all LDAP servers configured with the **ldap-server** command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the **aaa group server** command.

Example To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default group
ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default group
my_group
```

Note: This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

Related commands [aaa group server](#)
[download-portal](#)

Command changes Version 5.5.4-0: command added

aaa authentication enable default group tacacs+

Overview This command enables privilege level authentication against a TACACS+ server.

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

Syntax `aaa authentication enable default group tacacs+ [local] [none]`
`no aaa authentication enable default`

Parameter	Description
local	Use the locally configured enable password (enable password command) for authentication.
none	No authentication.

Default Local privilege level authentication is enabled by default (**aaa authentication enable default local** command).

Mode Global Configuration

Usage notes A user is configured on a TACACS+ server with a maximum privilege level. When they enter the **enable (Privileged Exec mode)** command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

NOTE: *If both are specified, you must always specify first.*

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**
then the user is never granted access to Privileged Exec mode.
- **aaa authentication enable default group tacacs+ local**
then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command), then the enable authentication will fail until the TACACS+ server becomes available again.
- **aaa authentication enable default group tacacs+ none**
then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.
- **aaa authentication enable default group tacacs+ local none**
then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

Examples To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

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

To disable privilege level authentication, use the following commands:

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

Related commands

- aaa authentication login**
- aaa authentication enable default local**
- enable (Privileged Exec mode)**
- enable password**
- enable secret (deprecated)**
- tacacs-server host**

aaa authentication enable default local

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

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

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

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

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

```
awplus# configure terminal
```

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

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

```
awplus# configure terminal
```

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

Related commands

- enable (Privileged Exec mode)**
- enable password**
- enable secret (deprecated)**

aaa authentication isakmp

Overview Use this command to enable global RADIUS authentication for ISAKMP tunnels.

Use the **no** variant of this command to disable global RADIUS authentication of ISAKMP tunnels.

Syntax `aaa authentication isakmp default group [<group-name>|radius]`
`no aaa authentication isakmp default`

Parameter	Description
<code><group-name></code>	Server group name
<code>radius</code>	Use all RADIUS servers

Default Disabled

Mode Global Configuration

Usage notes When RADIUS authentication is enabled globally to ISAKMP tunnels it is automatically applied to every ISAKMP tunnel interface.

There are two ways to define servers where radius accounting messages are sent:

- Group `radius`, where all RADIUS servers configured using this command are used
- Group `<group-name>`, where the specified RADIUS server group configured is used

Examples To enable RADIUS authentication for ISAKMP tunnels globally and use all available radius servers, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication isakmp default group radius
```

To disable RADIUS authentication for ISAKMP tunnels, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no authentication isakmp default
```

Related commands [radius-server host](#)
[aaa group server](#)

Command changes Version 5.4.9-0.1: command added

aaa authentication login

Overview Use this command to create an ordered list of methods for authenticating user logins. It can also be used to replace an existing method list with a list of the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the **login authentication** command. To apply a non-default method list, you must also use the **login authentication** command.

Use the **no** variant of this command to remove a method list from user login authentication. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

Syntax `aaa authentication login {default|<list-name>} {[local] [group {radius|ldap|tacacs+|<group-name>}]}`
`no aaa authentication login {default|<list-name>}`

Parameter	Description
default	Set the default authentication server for user login.
<list-name>	Name of authentication server.
local	Use the local username database.
group	Use server group.
radius	Use all RADIUS servers configured by the radius-server host command.
ldap	Use all LDAP servers configured by the ldap-server command.
tacacs+	Use all TACACS+ servers configured by the tacacs-server host command.
<group-name>	Use the specified RADIUS or LDAP server group.

Default If the default server is not configured using this command, user login authentication uses the local user database only.

If the **default** method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the **login authentication** command.

local is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. You can reset it to the default method list using the **no aaa authentication login default** command.

Mode Global Configuration

Usage notes When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies **group tacacs+ local**, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers nor the local user database; the user login fails.

Examples To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure the default authentication method list for user login to first use all available LDAP servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group ldap
local
```

To configure a user login authentication method list called 'USERS' to first use the RADIUS server group 'RAD_GROUP1' for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1
local
```

To configure a user login authentication method list called 'USERS' to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

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

To delete an existing authentication method list 'USERS' created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related commands [aaa accounting commands](#)
[aaa authentication enable default group tacacs+](#)
[ldap-server](#)
[login authentication](#)
[radius-server host](#)

Command changes Version 5.5.2-1.1: **ldap** parameter added

aaa authentication openvpn

Overview Use this command to globally enable authentication, and set the default authentication method, on OpenVPN tunnels. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

In addition, you can optionally specify that two-factor authentication (2FA) is required on OpenVPN connections.

Use the **no** variant of this command to globally disable authentication on OpenVPN tunnels.

Syntax `aaa authentication openvpn default group {<group-name>|radius|ldap} [2fa [2fa-in-password]]`
`no aaa authentication openvpn default`

Parameter	Description
<code><group-name></code>	Server group name.
<code>radius</code>	Use all RADIUS servers.
<code>ldap</code>	Use all LDAP servers.
<code>2fa</code>	Require two-factor authentication (2FA).
<code>2fa-in-password</code>	Include the 2FA verification code in the password.

Default Authentication on OpenVPN tunnels is disabled by default.

Mode Global Configuration

Usage notes There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the **radius-server host** command.
- **group ldap:** use all LDAP servers configured with the **ldap-server** command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the **aaa group server** command.

The **2fa** parameter allows you to strengthen security by requiring a second method of authentication. It requires a software-based authenticator that implements the time-based one-time password (TOTP) or HMAC-based one-time password (HOTP) algorithms. These software authenticators (known as authenticator apps) are usually loaded on a mobile device. One well-known implementation of such an app is Google Authenticator.

The **2fa-in-password** parameter allows the user to enter their 2FA authentication code straight after their password in the password field of the OpenVPN client. For example, if their password is 'secret' and their OpenVPN code is '654321', they will enter 'secret654321' into the OpenVPN client's password field.

Examples To enable RADIUS authentication on OpenVPN tunnels and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group radius
```

To enable authentication on OpenVPN tunnels using the servers in group 'GROUP2', use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group GROUP2
```

Note: This could be a group of RADIUS or LDAP servers.

To enable LDAP authentication on OpenVPN tunnels, use all available LDAP servers, and require 2FA with the 2FA code in the password field, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group ldap
                2fa 2fa-in-password
```

To disable authentication on OpenVPN tunnels, use the commands:

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

Related commands **aaa accounting openvpn**
aaa group server
radius-server host

Command changes Version 5.5.2-1.1: **ldap** and **2fa** parameters added

aaa authorization commands

Overview This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

Syntax `aaa authorization commands <privilege-level> {default|<list-name>} group tacacs+ [none]`
`no aaa authorization commands <privilege-level> {default|<list-name>}`

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: Level = 1: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive Level = 7: All commands that can be accessed by a user with privilege level between 7 and 14 inclusive Level = 15: All commands that can be accessed by a user with privilege level 15
group	Specify the server group where authorization messages are sent. Only the tacacs+ group is available for this command.
tacacs+	Use all TACACS+ servers configured by the tacacs-server host command.
default	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list
none	If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.

Mode Global Configuration

Usage notes TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.
- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

Example To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authorization commands 15 TAC15 group tacacs  
+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authorization commands 7 default group  
tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa authorization commands 15 TAC15
```

Related commands [aaa authorization config-commands](#)
[authorization commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

aaa authorization config-commands

Overview Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

Syntax `aaa authorization config-commands`
`no aaa authorization config-commands`

Default By default, command authorization is disabled on configuration mode commands.

Mode Global Configuration

Usage notes If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

NOTE: *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

Example To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

Related commands [aaa authorization commands](#)
[authorization commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

aaa group server

Overview Use this command to create an AAA group of RADIUS or LDAP servers, and to enter Server Group Configuration mode.

A server group is used to specify a subset of RADIUS or LDAP servers in AAA commands. Once in Server Group Configuration mode you can add servers to the group.

Use the **no** variant of this command to remove an existing server group.

Syntax `aaa group server {radius|ldap} <group-name>`
`no aaa group server {radius|ldap} <group-name>`

Parameter	Description
radius	Create or configure a RADIUS server group.
ldap	Create or configure an LDAP server group.
<group-name>	Server group name.

Mode Global Configuration

Usage notes To add servers to a RADIUS or LDAP server group, use the **server** command. Each RADIUS server in a server group must be configured using the **radius-server host** command. Similarly, each LDAP server in a server group must be configured using the **ldap-server** command.

Server groups named 'radius' and 'ldap' are predefined and include all RADIUS and LDAP servers configured using the **radius-server host** or **ldap-server** commands.

Examples To create a RADIUS server group named 'GROUP1' with hosts 192.168.1.1, 192.168.2.1 and 192.168.3.1, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named 'GROUP1' from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

To create an LDAP server group named 'GROUP2' with servers named 'SERVER1', 'SERVER2' and 'SERVER3', use the commands:

```
awplus(config)# aaa group server ldap GROUP2
awplus(config-ldap-group)# server SERVER1
awplus(config-ldap-group)# server SERVER2
awplus(config-ldap-group)# server SERVER3
```

To remove an LDAP server group named 'GROUP2' from the configuration, use the command:

```
awplus(config)# no aaa group server ldap GROUP2
```

Related commands

- ldap-server**
- radius-server host**
- server (ldap-group)**
- server (RADIUS server group)**
- show ldap server group**
- show radius server group**

Command changes Version 5.5.2-1.1: **ldap** parameter added

aaa local authentication attempts lockout-time

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

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

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

Parameter	Description
<code><lockout-time></code>	<code><0-10000></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 remote-login-only
clear aaa local user lockout

aaa local authentication attempts max-fail

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

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

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related commands **aaa local authentication attempts logout-time**
aaa local authentication attempts max-fail remote-login-only
clear aaa local user logout

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

Overview Use this command to configure account lockout to remote logins only. This means that console logins are not subject to lock out when this feature is configured.

This command allow users to login via the physical console port even when the account is locked due to reaching the maximum number of failed login attempts.

Use the **no** variant of this command to prevent users from logging in via the console port when the maximum number of failed login attempts is reached.

Syntax `aaa local authentication attempts max-fail remote-login-only`
`no aaa local authentication attempts max-fail remote-login-only`

Default Not set. Max-fail lockout applies to all logins.

Mode Global Configuration

Example To configure account lock-out to remote login only, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail
remote-login-only
```

To configure account lock-out to apply to all logins, use the commands:

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

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

Command changes Version 5.5.4-1.2: command added

aaa login fail-delay

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

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

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

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

Default 1 second

Mode Global configuration

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

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

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

accounting login

Overview This command applies a login accounting method list to console or VTY lines for user login. When login accounting is enabled using this command, logging events generate an accounting record to the accounting server.

The accounting method list must be configured first using this command. If an accounting method list is specified that has not been created by this command then accounting will be disabled on the specified lines.

The **no** variant of this command resets AAA Accounting applied to console or VTY lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

Syntax accounting login {default|<list-name>}
no accounting login

Parameter	Description
default	Default accounting method list.
<list-name>	Named accounting method list.

Default By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using this command.

Mode Line Configuration

Examples To apply the accounting server USERS to all VTY lines, use the following commands:

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

To reset accounting for login sessions on the console, use the following commands:

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

Related commands [aaa accounting commands](#)
[aaa accounting login](#)

authorization commands

Overview This command applies a command authorization method list, defined using the **aaa authorization commands** command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

Syntax authorization commands <privilege-level> {default|<list-name>}
no authorization commands <privilege-level>

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: Level = 1: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive Level = 7: All commands that can be accessed by a user with privilege level between 7 and 14 inclusive Level = 15: All commands that can be accessed by a user with privilege level 15
default	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list

Default The **default** method list is applied to each console and VTY line by default.

Mode Line Configuration

Usage notes If the specified method list does not exist users will not be able to execute any commands in the specified method list on the specified VTY lines.

Example To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

Related commands [aaa authorization commands](#)
[aaa authorization config-commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

clear aaa local user logout

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

Syntax clear aaa local user logout {username <username>|all}

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

Mode Privileged Exec

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

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

To unlock all user accounts use the following command:

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

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

debug aaa

Overview This command enables AAA debugging.

Use the **no** variant of this command to disable AAA debugging.

Syntax debug aaa [accounting|all|authentication|authorization]
no debug aaa [accounting|all|authentication|authorization]

Parameter	Description
accounting	Accounting debugging.
all	All debugging options are enabled.
authentication	Authentication debugging.
authorization	Authorization debugging.

Default AAA debugging is disabled by default.

Mode Privileged Exec

Examples To enable authentication debugging for AAA, use the command:

```
awplus# debug aaa authentication
```

To disable authentication debugging for AAA, use the command:

```
awplus# no debug aaa authentication
```

Related commands [show debugging aaa](#)
[undebug aaa](#)

login authentication

Overview Use this command to apply an AAA server for authenticating user login attempts from a console or remote logins on these console or VTY lines. The authentication method list must be specified by the **aaa authentication login** command. If the method list has not been configured by the **aaa authentication login** command, login authentication will fail on these lines.

Use the **no** variant of this command to reset AAA Authentication configuration to use the default method list for login authentication on these console or VTY lines.

Command login authentication {default|<list-name>}

Syntax no login authentication

Parameter	Description
default	The default authentication method list. If the default method list has not been configured by the aaa authentication login command, the local user database is used for user login authentication.
<list-name>	Named authentication server.

Default The default login authentication method list, as specified by the **aaa authentication login** command, is used to authenticate user login. If this has not been specified, the default is to use the local user database.

Mode Line Configuration

Examples To apply the authentication method list called CONSOLE to the console port terminal line (asyn 0), use the following commands:

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

To reset user authentication configuration on all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# no login authentication
```

Related commands **aaa authentication login**
line

proxy-port

Overview Use this command to change the local UDP port used for communication between local RADIUS client applications and the RadSecProxy AAA application. Any unused UDP port may be selected. The default port is 1645.

Use the **no** variant of this command to change the UDP port back to the default of 1645.

Syntax proxy-port <port>
no proxy-port

Parameter	Description
<port>	UDP Port Number, 1-65536.

Default The default port is 1645.

Mode RadSecProxy AAA Configuration Mode

Usage notes It is not necessary to change the value from the default unless UDP port 1645 is required for another purpose. RADIUS requests received on this port from external devices will be ignored. The port is only used for local (intra-device) communication.

Example To configure change the UDP port to 7001, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# proxy-port 7001
```

Related commands [radius-secure-proxy aaa](#)
[server \(radsecproxy-aaa\)](#)
[server name-check](#)
[server trustpoint](#)

radius-secure-proxy aaa

Overview Use this command to enter the RadSecProxy AAA (authentication, authorization, and accounting) application configuration mode. This application allows local RADIUS-based clients on system to communicate with remote RadSec servers via a secure (TLS) proxy.

Syntax radius-secure-proxy aaa

Mode Global Configuration Mode

Example To change mode from User Exec mode to the RadSecProxy AAA configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)#
```

Related commands

- proxy-port**
- server (radsecproxy-aaa)**
- server name-check**
- server trustpoint**

server (radsecproxy-aaa)

Overview Use this command to add a server to the RadSecProxy AAA application. Local RADIUS client applications will attempt, via the proxy, to communicate with any RadSec servers that are operational (in addition to any non-TLS RADIUS servers that are configured).

Use the **no** variant of this command to delete a previously-configured server from the RadSecProxy AAA application.

Syntax server {<hostname>|<ip-addr>} [timeout <1-1000>] [name-check {on|off}]
no server {<hostname>|<ip-addr>}

Parameter	Description
<hostname>	Hostname of RadSec server
	< Specify the client IPv4 address, in dotted decimal notation a (A.B.C.D).
	t Specify the amount of time that the RadSecProxy AAA application should wait for replies from this server. RADIUS server timeout (which defaults to 5 seconds).
	< Time in seconds to wait for a server reply.
	n Specify whether or not to enforce certificate name c checking for this client. If the parameter is not specified then the global behavior, which defaults to on , is used.
	Enable name checking for this client.
	Disable name checking for this client.

Mode RadSecProxy AAA Configuration Mode

Usage notes The server may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each server may be configured with a timeout; if not specified, the global timeout value for RADIUS servers will be used. The global timeout may be changed using the **radius-server timeout** command. The default global timeout is 5 seconds.

Each server may be configured to use certificate name-checking; if not specified, the global behavior defined by **server name-check** or **no server name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the server's X.509 certificate must match the domain name or IP address specified in this command.

Example To add a server 'mynas.local' with a timeout of 3 seconds, and name checking off, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# server mynas.local name-check
off
```

Related commands

- proxy-port**
- radius-secure-proxy aaa**
- server name-check**
- server trustpoint**

server mutual-authentication

Overview This command enables or disables mutual certificate authentication for all RadSecProxy servers. When enabled, the RadSecProxy AAA application will send a local X.509 certificate to the server when establishing a TLS connection.

Use the **no** variant of this command to disable mutual certificate validation causing the RadSecProxy AAA application to not transmit a certificate to the server.

NOTE: *If mutual authentication is disabled on the client (AAA) application but enabled on the server, a connection will not be established.*

Syntax server mutual-authentication
no server mutual-authentication

Default Mutual authentication is enabled by default.

Mode RadSecProxy AAA Configuration Mode

Example Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server mutual-authentication
```

Related commands [radius-secure-proxy aaa](#)
[server name-check](#)
[server \(radsecproxy-aaa\)](#)

Command changes Version 5.4.6-2.1: command added

server name-check

Overview This command sets the global behavior for certificate name-checking for the RadSecProxy AAA application to **on**. This behavior will be used for all servers associated with the application that do not specify a behavior on a per-server basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **server (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

Syntax server name-check
no server name-check

Default Certificate name checking is on by default.

Mode RadSecProxy AAA Configuration Mode

Example Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server name-check
```

Related commands [proxy-port](#)
[radius-secure-proxy aaa](#)
[server \(radsecproxy-aaa\)](#)
[server trustpoint](#)

server trustpoint

Overview This command adds one or more trustpoints to be used with the RadSecProxy AAA application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax `server trustpoint [<trustpoint-list>]`
`no server trustpoint [<trustpoint-list>]`

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Default By default, no trustpoints are associated with the application.

Mode RadSecProxy AAA Configuration Mode

Usage notes The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no server trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints to the RadSecProxy AAA application by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radius-secure-proxy-aaa)# server trustpoint example_1
awplus(config-radius-secure-proxy-aaa)# server trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radius-secure-proxy-aaa)# server trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy AAA application using the command:

```
awplus(config-radius-secure-proxy-aaa)# no server trustpoint
```

Related **proxy-port**
commands **radius-secure-proxy aaa**
server (radsecproxy-aaa)
server name-check

show aaa local user locked

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

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

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

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

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

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

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

In the Valid column:

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

Syntax show aaa local user locked

Mode User Exec and Privileged Exec

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

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

Output The following shows typical output.

Example output from the show aaa local user locked command

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

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

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

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

show aaa server group

Overview Use this command to list AAA users and any method lists applied to them.

Syntax show aaa server group

Mode Privileged Exec

Example To show the AAA configuration on a device, use the command:

```
awplus# show aaa server group
```

Output The following shows typical output.

Example output from show aaa server group

awplus#show aaa server group					
User		List Name	Method		Acct-Event
=====	=====	=====	=====	=====	=====
login	auth	default	-	local	-
-----	-----	-----	-----	-----	-----
cmd-1	auth	-	-	-	-
-----	-----	-----	-----	-----	-----
cmd-7	auth	-	-	-	-
-----	-----	-----	-----	-----	-----
cmd-15	auth	-	-	-	-
-----	-----	-----	-----	-----	-----
login	acct	-	-	-	-
-----	-----	-----	-----	-----	-----
openvpn	auth	-	-	-	-
-----	-----	-----	-----	-----	-----
isakmp	auth	default	radius	group	-
-----	-----	-----	-----	-----	-----

show debugging aaa

Overview Use this command to see what debugging is turned on for AAA (Authentication, Authorization, Accounting).

Syntax show debugging aaa

Mode User Exec and Privileged Exec

Example To display the current debugging status of AAA, use the command:
awplus# show debug aaa

Output The following shows typical output.

Example output from the show debug aaa command

```
AAA debugging status:  
Authentication debugging is on  
Accounting debugging is off
```

show radius server group

Overview Use this command to show the RADIUS server group configuration.

Syntax show radius server group [*<group-name>*]

Parameter	Description
<i><group-name></i>	RADIUS server group name.

Default Command name is set to something by default.

Mode Privileged Exec

Usage Use this command with the *<group-name>* parameter to display information for a specific RADIUS server group, or without the parameter to display information for all RADIUS server groups.

Example To display information for all RADIUS server groups, use the command:

```
awplus# show radius server group
```

To display a information for a RADIUS server group named 'rad_group_list1', use the command:

```
awplus# show radius server group rad_group_list1
```

Output The following shows typical output.

Example output from show radius server group

```
awplus#show radius server group
RADIUS Group Configuration
  Group Name : radius#
    Server Host/   Auth  Acct  Auth  Acct
    IP Address     Port  Port  Status Status
    -----
    192.168.1.101  1812 1813  Active Active
    192.168.1.102  1812 1813  Active Active

  Group Name : rad_group_list1
    Server Host/   Auth  Acct  Auth  Acct
    IP Address     Port  Port  Status Status
    -----
    192.168.1.101  1812 1813  Active Active

  Group Name : rad_group_list2
    Server Host/   Auth  Acct  Auth  Acct
    IP Address     Port  Port  Status Status
    -----
    192.168.1.102  1812 1813  Active Active
```

Example output from show radius server group rad_group_list1

```
awplus#show radius server group rad_group_list1
RADIUS Group Configuration
  Group Name : rad_group_list1
    Server Host/   Auth  Acct  Auth  Acct
    IP Address     Port  Port  Status Status
    -----
    192.168.1.101  1812 1813  Active Active
```

Related commands [aaa group server](#)

undebug aaa

Overview This command applies the functionality of the **no debug aaa** .

23

Lightweight Directory Access Protocol (LDAP) Commands

- Contents**
- **Introduction** on page 1082
 - **authentication (ldap-server)** on page 1083
 - **base-dn** on page 1085
 - **bind authenticate root-dn** on page 1087
 - **deadtime (ldap-server)** on page 1088
 - **debug ldap client** on page 1089
 - **group-attribute** on page 1091
 - **group-dn** on page 1092
 - **host (ldap-server)** on page 1093
 - **ldap-server** on page 1095
 - **login-attribute** on page 1097
 - **port (ldap-server)** on page 1099
 - **retransmit (ldap-server)** on page 1101
 - **search-filter** on page 1102
 - **secure cipher (ldap-server)** on page 1104
 - **secure mode (ldap-server)** on page 1106
 - **secure trustpoint (ldap-server)** on page 1108
 - **server (ldap-group)** on page 1109
 - **show ldap server group** on page 1110
 - **timeout (ldap-server)** on page 1112

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Lightweight Directory Access Protocol (LDAP).

LDAP is an authentication protocol that facilitates user access to various IT resources e.g. applications, servers, networking equipment, and file servers.

It can be used to connect to internal networks over OpenVPN. Although both LDAP and RADIUS are interchangeable on AlliedWare Plus devices as an authentication protocol, LDAP is added because of its ability to interact with directory services such as Microsoft's Active Directory (AD).

For more information, see the **LDAP Feature Overview and Configuration Guide**.

authentication (ldap-server)

Overview Use this command to set the authentication method used to authenticate users against the Lightweight Directory Access Protocol (LDAP) server.

Use the **no** variant of this command to reset the authentication method to **search**.

Syntax authentication {search|bind-only}
no authentication

Parameter	Description
search	The search method initially binds to the LDAP server, then searches for the user, then binds to the user using the DN found with the search. The initial bind is either anonymous, or using the user specified with the bind authenticate root-dn command.
bind-only	The bind-only method attempts to bind to the LDAP server using a predicted DN based on the username, the user attribute (set with the login-attribute command) and the base DN (set with the base-dn command). The format of this user DN is as follows: '<username>=<login-attribute>,<base-dn>'.

Default Search

Mode LDAP Server Configuration

Example To set the authentication method to bind-only for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# authentication bind-only
```

To reset the authentication method to the default (search) for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no authentication
```

Related commands **base-dn**
 bind authenticate root-dn
 ldap-server
 login-attribute
 search-filter

Command changes Version 5.5.2-1.1: command added

base-dn

Overview Use this command to set the base DN (Distinguished Name) of the LDAP server.

When using 'search' authentication, the base DN is the LDAP server's starting point to search for the user within the directory.

If 'bind-only' authentication is enabled, then the base DN is the suffix of the DN that is used to bind to the user.

Use the **no** variant of this command to remove the configured base DN.

Syntax base-dn <base-dn>
no base-dn

Parameter	Description
<base-dn>	The base DN of the LDAP server.

Default Not set

Mode LDAP Server Configuration

Example To set the base DN for the LDAP server called 'Server1' to 'dc=example, dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# base-dn dc=example,dc=com
```

To clear the base DN for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no base-dn
```

Related commands

- [authentication \(ldap-server\)](#)
- [bind authenticate root-dn](#)
- [group-attribute](#)
- [group-dn](#)
- [ldap-server](#)
- [login-attribute](#)
- [search-filter](#)

Command changes Version 5.5.2-1.1: command added

bind authenticate root-dn

Overview Use this command to set the authenticated user to bind to when searching for a user on an LDAP server. Do not set this option if you wish to use anonymous binding with the 'search' method.

This option is ignored with the 'bind-only' authentication method.

Use the **no** variant of this command to unset the authenticated user.

Syntax bind authenticate root-dn <user-dn> password <password>
no bind authenticate root-dn

Parameter	Description
<user-dn>	The DN of the authenticated user to bind to.
<password>	The password of the authenticated user.

Default Not set

Mode LDAP Server Configuration

Example To set the authenticated user to 'cn=admin,dc=example,dc=com' with the password '12345678' for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# bind authenticate root-dn
cn=admin,dc=example,dc=com password 12345678
```

Related commands [authentication \(ldap-server\)](#)
[base-dn](#)
[group-attribute](#)
[ldap-server](#)
[login-attribute](#)
[search-filter](#)

Command changes Version 5.5.2-1.1: command added

deadtime (ldap-server)

Overview Use this command to configure the deadtime for an LDAP server. The configured deadtime is how long in seconds before an unresponsive LDAP server is considered dead.

Use the **no** variant of this command to remove the deadtime configured on an LDAP server. When you remove the deadtime, the server will never be considered dead.

Syntax deadtime <0-1440>
no deadtime

Parameter	Description
<0-1440>	The number of seconds that the server can be unresponsive for before it is considered dead.

Default 0 seconds (the LDAP server is never considered dead)

Mode LDAP Server Configuration

Example To set the deadtime to 20 seconds for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# deadtime 20
```

To reset the deadtime to the default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no deadtime
```

Related commands [host \(ldap-server\)](#)
[ldap-server](#)
[port \(ldap-server\)](#)
[retransmit \(ldap-server\)](#)
[show ldap server group](#)
[timeout \(ldap-server\)](#)

Command changes Version 5.5.2-1.1: command added

debug ldap client

Overview Use this command to enable LDAP debugging.
Use the **no** variant of this command to disable all LDAP debugging.

Syntax debug ldap client all
debug ldap client {[args] [ber] [config] [conns] [filter]
[packets] [parse] [shell] [stats] [stats2] [sync] [trace]}
no debug ldap client

Parameter	Enable or disable debugging for ...
all	All LDAP debugging options
args	Heavy trace debugging (args, arguments)
ber	Print out packets sent and received (ber, Bit Error Rate)
config	Configuration processing
conns	Connection management
filter	Search filter processing
packets	Debug packet handling
parse	Parsing processing
shell	Print communication with shell backends
stats	Stats from connections, operations and results
stats2	Stats from log entries sent
sync	Syncrepl consumer processing (LDAP Sync replication)
trace	Trace function calls

Default By default, all LDAP debugging is disabled.

Mode Global Configuration

Example To turn on all LDAP debugging, use the command:

```
awplus# debug ldap client all
```

To turn on filter and packet LDAP debugging, use the command:

```
awplus# debug ldap client filter packets
```

To disable all LDAP debugging, use the command:

```
awplus# no debug ldap client
```

Related commands [aaa authentication openvpn](#)
[aaa group server](#)
[ldap-server](#)

Command changes Version 5.5.2-1.1: command added

group-attribute

Overview Use this command to configure the name of the attribute that group members are stored in.

It is only necessary to set this option if **group-dn** is used and you don't want to use the default attribute, which is 'uniquemember'.

Use the **no** variant of this command to revert to the default group attribute.

Syntax group-attribute <attribute>
no group-attribute

Parameter	Description
<attribute>	The attribute that group members are stored in.

Default The default group attribute is 'uniquemember'.

Mode LDAP Server Configuration

Example To set the group attribute for the LDAP server called 'Server1' to 'member', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-attribute member
```

To reset the group attribute to default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-attribute
```

Related commands

- base-dn**
- bind authenticate root-dn**
- group-dn**
- ldap-server**
- login-attribute**
- search-filter**

Command changes Version 5.5.2-1.1: command added

group-dn

Overview Use this command to configure the group DN (Distinguished Name) of the group that users should be a member of.

By default the device will determine this by checking the 'uniquemember' attribute of the group to see if it contains the user's DN string. This can be changed with the **group-attribute** command.

Use the **no** variant of this command to remove the configured group DN.

Syntax group-dn <group-dn>
no group-dn

Parameter	Description
<group-dn>	The DN of the group that users should be a member of.

Default Not set

Mode LDAP Server Configuration

Example To set the group DN for the LDAP server called 'Server1' to 'cn=Users,dc=example,dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-dn cn=Users,dc=example, dc=com
```

To clear the group DN for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-dn
```

Related commands **base-dn**
bind authenticate root-dn
group-attribute
ldap-server
login-attribute
search-filter

Command changes Version 5.5.2-1.1: command added

host (ldap-server)

Overview Use this command to configure the address of the remote LDAP server you want to connect to.

Use the **no** variant of this command to remove the remote LDAP server.

Syntax host {<host-name>|<ip-address>|<ipv6-address>}
no host

Parameter	Description
<hostname>	The hostname of the LDAP server.
<ip-address>	The IPv4 address of the LDAP server. Uses the format A.B.C.D.
<ipv6-address>	The IPv6 address of the LDAP server. Uses the format x:x::x:x.

Default Not set

Mode LDAP Server Configuration

Example To set the host for the LDAP server called 'Server1' to the IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 10.0.0.1
```

To set the host for Server1 to the IPv6 address 2001:0db8::a2, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 2001:db8::a2
```

To set the host for Server1 to the hostname www.ldapserver.com, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host www.ldapserver.com
```

To unset the host for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no host
```

Related commands **ldap-server**
port (ldap-server)
retransmit (ldap-server)
secure mode (ldap-server)
secure cipher (ldap-server)
show ldap server group
secure trustpoint (ldap-server)
timeout (ldap-server)

Command changes Version 5.5.2-1.1: command added

ldap-server

Overview Use this command to configure an LDAP server and enter LDAP server configuration mode.

Use the **no** variant of this command to remove the specified server.

Syntax ldap-server <server-name>
no ldap-server <server-name>

Parameter	Description
<server-name>	The name of the LDAP server.

Default Not set

Mode Global Configuration

Example To create and configure an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To configure the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To remove an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# no ldap-server Server1
```

Related commands

- [authentication \(ldap-server\)](#)
- [host \(ldap-server\)](#)
- [port \(ldap-server\)](#)
- [retransmit \(ldap-server\)](#)
- [secure cipher \(ldap-server\)](#)
- [secure mode \(ldap-server\)](#)
- [secure trustpoint \(ldap-server\)](#)
- [show ldap server group](#)
- [timeout \(ldap-server\)](#)

Command changes Version 5.5.2-1.1: command added

login-attribute

Overview Use this command to set the name of the attribute user names are stored in. The device will search this attribute for the user's DN (Distinguished Name).

It is only necessary to set this option if you don't want to use the default attribute, which is 'uid'.

If the authentication method is 'bind-only', then this attribute is used as the first component of the user DN, with the base DN added to complete the user DN.

Use the **no** variant of this command to reset the login attribute to the default of 'uid'.

Syntax login-attribute <attribute>
no login-attribute

Parameter	Description
<attribute>	The LDAP attribute to use for the username of connecting users.

Default uid

Mode LDAP Server Configuration

Example To set the login attribute for the LDAP server called 'Server1' to 'sAMAccountName', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# login-attribute sAMAccountName
```

To reset the login attribute for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no login-attribute
```

Related command **authentication (ldap-server)**
base-dn
bind authenticate root-dn
group-attribute
group-dn
ldap-server
search-filter

Command changes Version 5.5.2-1.1: command added

port (ldap-server)

Overview Use this command to configure the port you are using to connect to the remote LDAP server.

Note that if secure ciphers are enabled, then the secure port is used instead. Secure ciphers are configured with the **secure mode (ldap-server)** command.

Use the **no** variant of this command to reset the port number to the default (389).

Syntax port <1-65535>
no port

Parameter	Description
<1-65535>	Port number from 1 through 65535.

Default 389

Mode LDAP Server Configuration

Example To set the port for the LDAP server called 'Server1' to 1579, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# port 1579
```

To reset the port for 'Server1' to the default of 389, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no port
```

Related commands	deadtime (ldap-server)
	host (ldap-server)
	ldap-server
	retransmit (ldap-server)
	secure cipher (ldap-server)
	secure mode (ldap-server)
	secure trustpoint (ldap-server)
	show ldap server group
Command changes	timeout (ldap-server)
	Version 5.5.2-1.1: command added

retransmit (ldap-server)

Overview Use this command to configure the number of times a device will attempt to reconnect to the LDAP server before aborting.

Use the **no** variant of this command to reset the reconnect attempts to the default value of 3.

Syntax retransmit <0-100>
no retransmit

Parameter	Description
<0-100>	The number of times the device will attempt to reconnect to the LDAP server.

Default 3 times

Mode LDAP Server Configuration

Example To set the number of reconnect attempts for the LDAP server called 'Server1' to 5 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# retransmit 5
```

To reset the number of reconnect attempts for 'Server1' to 3 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no retransmit
```

Related commands [deadtime \(ldap-server\)](#)
[host \(ldap-server\)](#)
[ldap-server](#)
[port \(ldap-server\)](#)
[timeout \(ldap-server\)](#)

Command changes Version 5.5.2-1.1: command added

search-filter

Overview Use this command to add a filter to use when searching for a user on the LDAP server.

The filter should be a form similar to 'attribute=value' or '&(attribute1=value1)(attribute2=value2)

Use the **no** variant of this command to remove the search filter.

Syntax search-filter <filter>
no search-filter

Parameter	Description
<filter>	The filter to use when searching for a user.

Default Not set

Mode LDAP Server Configuration

Usage notes If the 'bind-only' authentication method is used, then this value is unused.
For the search authentication method, a search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

Example To set a search filter on the LDAP server called 'Server1' to 'building=block1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# search-filter building=block1
```

To unset the search filter of 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no search-filter
```

Related commands **authentication (ldap-server)**
base-dn
bind authenticate root-dn
group-attribute
group-dn
ldap-server
login-attribute

Command changes Version 5.5.2-1.1: command added

secure cipher (ldap-server)

Overview Use this command to configure the OpenSSL ciphers used in LDAP secure mode. You can choose groups of ciphers from a number of Mozilla TLS configs, or specify multiple individual ciphers in OpenSSL format.

Use the **no** variant of this command to remove the configured ciphers on a server.

Syntax secure cipher {old|intermediate|modern}
secure cipher <cipher-list>
no secure cipher

Parameter	Description
old	Ciphers in Mozilla's old TLS config. Alongside the modern and intermediate ciphers, this includes the following ciphers: DHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-AES128SHA256, ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA,DHE-RSA-AES128-SHA256, DHE-RSA-AES256-SHA256, AES128-GCM-SHA256, AES256-GCM-SHA384,AES128-SHA256, AES256-SHA256, AES128-SHA, AES256-SHA, DES-CBC3-SHA
intermediate	Ciphers in Mozilla's intermediate TLS config. Alongside the modern ciphers, this includes the following ciphers: ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-CM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-CM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384
modern	Ciphers in Mozilla's modern TLS config. Includes the following ciphers: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256
<cipher-list>	The name (or names) of a cipher in OpenSSL format. This is a space separated list of cipher names, for example: DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384

Default Not set

Mode LDAP Server Configuration

Example To use the Intermediate Mozilla cipher suite on the LDAP server called Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher intermediate
```

To remove the configured ciphers on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure cipher
```

To use the ciphers DHE-DSS-AES256-GCM-SHA384 and TLS_AES_256_GCM_SHA384 on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384
```

Related commands

- [**host \(ldap-server\)**](#)
- [**ldap-server**](#)
- [**port \(ldap-server\)**](#)
- [**secure mode \(ldap-server\)**](#)
- [**secure trustpoint \(ldap-server\)**](#)

Command changes Version 5.5.2-1.1: command added

secure mode (ldap-server)

Overview Use this command to configure the LDAP server to use secure mode. Secure mode encrypts communications with the LDAP server using TLS (Transport Layer Security). If you don't specify a port number, the default port (636) is used.

For secure mode, you should also set the CA certificate using the **secure trustpoint (ldap-server)** command.

Use **no secure mode** to disable secure mode for communicating with this LDAP server.

Use **no secure mode secure-port** to reset the secure mode port to the default.

Syntax secure mode [secure-port <port>]
no secure mode
no secure mode secure-port

Parameter	Description
<port>	The secure port for communicating with the LDAP server

Default Secure mode is disabled, and the default port is 636

Mode LDAP Server Configuration

Example To enable secure mode for communicating with the LDAP server called 'Server1', with the default port, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode
```

To disable secure mode for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode
```

To enable secure mode with the port 1234 for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode secure-port 1234
```

To reset the secure mode port to the default on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode secure-port
```

Related commands

- host (ldap-server)**
- ldap-server**
- port (ldap-server)**
- secure cipher (ldap-server)**
- secure trustpoint (ldap-server)**

Command changes Version 5.5.2-1.1: command added

secure trustpoint (ldap-server)

Overview Use this command to link a preconfigured trustpoint to the LDAP server configuration. The trustpoint must be the LDAP server certificate and is required to successfully connect to the LDAP server when secure mode is enabled.

Use the **no** variant of this command to remove a trustpoint from an LDAP server.

Syntax secure trustpoint <trustpoint>
no secure trustpoint

Parameter	Description
<trustpoint>	The name of the trustpoint used for LDAP secure mode

Default Not set

Mode LDAP Server Configuration

Example To set the trustpoint to Trustpoint1 for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# secure trustpoint Trustpoint1
```

To remove the trustpoint from 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# no secure trustpoint
```

Related commands [host \(ldap-server\)](#)
[ldap-server](#)
[port \(ldap-server\)](#)
[secure cipher \(ldap-server\)](#)
[secure mode \(ldap-server\)](#)

Command changes Version 5.5.2-1.1: command added

server (ldap-group)

Overview Use this command to add an LDAP server to an LDAP server group. The server is identified by the name of the server, which is created using the **ldap-server** command. Use the **no** variant of this command to remove an LDAP server from an LDAP server group.

Syntax server <server-name>
no server <server-name>

Parameter	Description
<server-name>	The name of the LDAP server group, specified when creating the LDAP server.

Default By default, LDAP servers are only added to the default 'ldap' server group.

Mode LDAP Server Group Configuration

Usage notes The server is appended to the server list of the group, and the order of configuration determines the precedence of servers.

Example To add the LDAP server called 'Server1' to the LDAP server group called 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# server Server1
```

To remove 'Server1' from 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# no server Server1
```

Related commands [aaa authentication openvpn](#)
[aaa group server](#)
[ldap-server](#)
[show ldap server group](#)

Command changes Version 5.5.2-1.1: command added

show ldap server group

Overview Use this command to display information about LDAP server groups, their servers and the status of those servers.

Syntax show ldap server group [*<group-name>*]

Parameter	Description
<i><group-name></i>	The name of the LDAP server group.

Mode Global Configuration

Usage notes If you specify a single group name, you will only see information relating to that specific server group. Otherwise, all LDAP server groups are shown, including the 'ldap' group that contains every LDAP server.

Example To show all server groups, use the command:

```
awplus# show ldap server group
```

To show the default LDAP group that includes all the LDAP servers, use the command:

```
awplus# show ldap server group ldap
```

To show a server group named 'CustomGroup1', use the command:

```
awplus# show ldap server group CustomGroup1
```

Output The following shows typical output.

Example output from show ldap server group

```
LDAP Group Configuration
Group Name : ldap
LDAP server name  Server Host/IP Address  Port  Status
-----
server_one       10.1.1.1      N/A   Alive
server_two       10.2.1.1      N/A   Dead (1 hour)

Group Name : CustomGroup1
LDAP server name  Server Host/IP Address  Port  Status
-----
server_one       10.1.1.1      N/A   Alive

Group Name : CustomGroup2
LDAP server name  Server Host/IP Address  Port  Status
-----
No LDAP servers currently defined
```

Related commands [aaa authentication openvpn](#)
[aaa group server](#)
[deadtime \(ldap-server\)](#)
[ldap-server](#)
[port \(ldap-server\)](#)
[server \(ldap-group\)](#)

Command changes Version 5.5.2-1.1: command added

timeout (ldap-server)

Overview Use this command to set the time to wait for a connection before reattempting to connect to the LDAP server.

Use the **no** variant of this command to reset the timeout back to the default value.

Syntax timeout <1-1000>
no timeout

Parameter	Description
<1-1000>	The number of seconds to wait for a connection before reattempting to connect to the LDAP server.

Default 5 seconds

Mode LDAP Server Configuration

Example To set the server timeout for the LDAP server called 'Server1' to 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# timeout 10
```

To set the server timeout for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no timeout
```

Related commands [deadtime \(ldap-server\)](#)
[host \(ldap-server\)](#)
[ldap-server](#)
[port \(ldap-server\)](#)
[retransmit \(ldap-server\)](#)

Command changes Version 5.5.2-1.1: command added

24

RADIUS Commands

- Contents**
- **Introduction** on page 1114
 - **auth-mac-promiscuous** on page 1115
 - **deadtime (RADIUS server group)** on page 1116
 - **debug radius** on page 1117
 - **ip radius require-message-authenticator** on page 1118
 - **ip radius source-interface** on page 1119
 - **radius-server deadtime** on page 1120
 - **radius-server host** on page 1121
 - **radius-server key** on page 1126
 - **radius-server retransmit** on page 1128
 - **radius-server timeout** on page 1130
 - **server (RADIUS server group)** on page 1132
 - **show debugging radius** on page 1135
 - **show radius** on page 1136
 - **show radius local-server auth-mac-promiscuous** on page 1139
 - **undebg radius** on page 1140

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device as a RADIUS client.

For more information, see the **[RADIUS Feature Overview and Configuration Guide](#)**.

auth-mac-promiscuous

Overview Use this command to enable promiscuous mode for MAC address authentication on a local RADIUS server.

Use the **no** variant of this command to disable MAC authentication promiscuous mode on a local RADIUS server.

Syntax auth-mac-promiscuous
no auth-mac-promiscuous

Default Disabled.

Mode RADIUS Server Configuration

Usage notes In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

Example To disable MAC authentication promiscuous mode on a local RADIUS server, use the commands:

```
awplus# radius-server local  
awplus(config-radsrv)# no auth-mac-promiscuous
```

Related commands [show radius local-server auth-mac-promiscuous](#)

Command changes Version 5.5.3-2.1: command added

deadtime (RADIUS server group)

Overview Use this command to configure the **deadtime** parameter for the RADIUS server group. This command overrides the global dead-time configured by the **radius-server deadtime**. The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is 'dead'. Note that a RADIUS server is considered 'dead' if there is no response from the server within a defined time period.

Use the **no** variant of this command to reset the deadtime configured for the RADIUS server group. If the global deadtime for RADIUS server is configured the value will be used for the servers in the group. The global deadtime for the RADIUS server is set to 0 minutes by default.

Syntax `deadtime <0-1440>`
`no deadtime`

Parameter	Description
<code><0-1440></code>	Amount of time in minutes.

Default The deadtime is set to 0 minutes by default.

Mode RADIUS Server Group Configuration

Usage If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked 'dead', and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

Examples To configure the deadtime for 5 minutes for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

Related commands **aaa group server**
radius-server deadtime

debug radius

Overview This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

Syntax debug radius [packet|event|all]
no debug radius [packet|event|all]

Parameter	Description
packet	Debugging for RADIUS packets is enabled or disabled.
event	Debugging for RADIUS events is enabled or disabled.
all	Enable or disable all debugging options.

Default RADIUS debugging is disabled by default.

Mode Privileged Exec

Examples To enable debugging for RADIUS packets, use the command:

```
awplus# debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus# debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

Related commands [show debugging radius](#)
[undebug radius](#)

ip radius require-message-authenticator

Overview Use this command to configure the RADIUS client to reject unverified RADIUS packets. This means it will discard any received RADIUS Access-Accept, Access-Challenge, and Access-Reject packets that do not have a valid Message-Authenticator attribute.

Use the **no** variant of this command to allow the client to accept unverified RADIUS packets.

Syntax `ip radius require-message-authenticator`
`no ip radius require-message-authenticator`

Default Disabled

Mode Global Configuration

Example To require Message-Authenticator attributes in responses from RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# ip radius require-message-authenticator
```

Related commands [nas message-authenticator \(radsvr\)](#)
[radius-server host](#)
[show radius local-server nas](#)

Command changes Version 5.5.4-2.3: command added

ip radius source-interface

Overview This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

Syntax `ip radius source-interface {<interface>|<ip-address>}`
`no ip radius source-interface`

Parameter	Description
<code><interface></code>	Interface name.
<code><ip-address></code>	IP address in the dotted decimal format A.B.C.D.

Default Source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Mode Global Configuration

Examples To configure all outgoing RADIUS packets to use the IP address of the interface eth1 for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface eth1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

Related commands [radius-server host](#)

radius-server deadtime

Overview Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

Syntax radius-server deadtime <minutes>
no radius-server deadtime

Parameter	Description
<minutes>	RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).

Default The default RADIUS deadtime configured on the system is 0 seconds.

Mode Global Configuration

Usage The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the **radius-server retransmit** command or for the server by the **radius-server host** command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

Examples To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

Related commands **deadtime (RADIUS server group)**
radius-server host
radius-server retransmit

radius-server host

Overview Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [encrypted] [retransmit <0-100>] [timeout <1-1000>]
no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>]

Syntax (VRF-lite) radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [encrypted] [retransmit <0-100>] [timeout <1-1000>] [vrf <vrf-name>]
no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [vrf <vrf-name>]

Parameter	Description
<i><host-name></i>	Server host name. The DNS name of the RADIUS server host.
<i><ip-address></i>	The IP address of the RADIUS server host.
acct-port	Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.
<i><0-65535></i>	UDP port number. (Accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting.
auth-port	Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.
<i><0-65535></i>	UDP port number (authentication port number is set to 1812 by default). Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.
timeout	Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the radius-server timeout command is used.
<i><1-1000></i>	Time in seconds to wait for a server reply (timeout is set to 5 seconds by default). The time interval (in seconds to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the radius-server timeout command. If no timeout value is specified for this server, the global value is used.
retransmit	Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the radius-server retransmit command is used.
<i><0-100></i>	Maximum number of retries (maximum number of retries is set to 3 by default). The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the radius-server retransmit command. If no retransmit value is specified, the global value is used.

Parameter	Description
key	Set shared secret key with RADIUS servers.
<key-string>	Shared key string applied. Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored. This setting overrides the global setting of the radius-server key command. If no key value is specified, the global value is used.
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.
vrf <vrf-name>	The name of a VRF instance. Use this to specify the VRF that the RADIUS server is accessible by. Servers are uniquely identified by their address and VRF, so multiple servers can have the same address or host-name as long as the VRF is different. The default is the global VRF.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius-server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the **auth-port** parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret
```

To delete the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure rad1.company.com for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server rad1.company.com configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com acct-port
0
```

To configure rad2.company.com for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Examples (VRF-lite) To add the RADIUS server 10.0.0.20 in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 vrf red
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20 in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret vrf
red
```


Related commands **aaa group server**
 radius-server key
 radius-server retransmit
 radius-server timeout

Command changes Version 5.5.3-2.1: **encrypted** parameter added
 Version 5.5.2-1.1: **vrf** parameter added for products that support VRF
 Version 5.4.9-2.1: **key-encrypted** parameter added

radius-server key

Overview This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

Syntax radius-server key <key-string> [encrypted]
no radius-server key

Parameter	Description
<key-string>	Shared secret among RADIUS server and 802.1X client.
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.

Default The RADIUS server secret key on the system is not set by default (null).

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its RADIUS servers. If no secret key is specified for a particular RADIUS server using the **radius-server host** command, this global key is used.

After enabling AAA authentication with the **aaa authentication login** command, set the authentication and encryption key using the **radius-server key** command so the key entered matches the key used on the RADIUS server.

Examples To set the global secret key to **allied** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key allied
```

To set the global secret key to **secret** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key secret
```

To delete the global secret key for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server key
```

Related commands [radius-server host](#)

Command changes Version 5.5.3-2.1: **encrypted** parameter added

radius-server retransmit

Overview This command sets the retransmit counter to use RADIUS authentication on the device. This command specifies how many times the device transmits each RADIUS request to the RADIUS server before giving up.

This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.

Use the **no** variant of this command to reset the re-transmit counter to the default (3).

Syntax radius-server retransmit <retries>
no radius-server retransmit

Parameter	Description
<retries>	RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the radius-server host command, this global value is used.

Default The default RADIUS retransmit count on the device is 3.

Mode Global Configuration

Examples To set the RADIUS **retransmit** count to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 1
```

To set the RADIUS **retransmit** count to the default (3), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server retransmit
```

To configure the RADIUS **retransmit** count globally with 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 5
```

To disable retransmission of requests to a RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 0
```

Related commands [radius-server deadtime](#)
[radius-server host](#)

radius-server timeout

Overview Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax radius-server timeout <seconds>
no radius-server timeout

Parameter	Description
<seconds>	RADIUS server timeout in seconds in the range 1 to 1000. The global time in seconds to wait for a RADIUS server to reply to a request before retransmitting the request, or considering the server to be dead (depending on the radius-server retransmit command).

Default The default RADIUS transmit timeout on the system is 5 seconds.

Mode Global Configuration

Examples To globally set the device to wait 20 seconds before retransmitting a RADIUS request to unresponsive RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 20
```

To set the RADIUS **timeout** parameter to 1 second, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 1
```

To set the RADIUS **timeout** parameter to the default (5 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

To configure the RADIUS server **timeout** period globally with 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 3
```

To reset the global **timeout** period for RADIUS servers to the default, use the following command:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

Related commands [radius-server deadtime](#)
[radius-server host](#)
[radius-server retransmit](#)

server (RADIUS server group)

Overview This command adds a RADIUS server to a server group in RADIUS Server Group Configuration mode. The RADIUS server should be configured by the **radius-server host** command.

The device adds each server to the end of the group's list of servers, so add the servers in order of priority. If you add a server and it is already in the list, it will be removed and then re-added to the end of the list.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set **auth-port** to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set **acct-port** to 0. If the accounting port is missing, the default port number is 1813.

Use the **no** variant of this command to remove a RADIUS server from the server group.

Syntax `server {<hostname>|<ip-address>} [auth-port <0-65535>] [acct-port <0-65535>]`
`no server {<hostname>|<ip-address>} [auth-port <0-65535>] [acct-port <0-65535>]`

Parameter	Description
<hostname>	Server host name
<ip-address>	Server IP address The server is identified by IP address, authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports.
auth-port	Authentication port The auth-port specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set auth-port to 0. If the authentication port is missing, the default port number is 1812.
<0-65535>	UDP port number (default: 1812)
acct-port	Accounting port The acct-port specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set acct-port to 0. If the accounting port is missing, the default port number is 1813.
<0-65535>	UDP port number (default: 1813)

Default The default Authentication port number is 1812 and the default Accounting port number is 1813.

Mode RADIUS Server Group Configuration

Usage notes The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the **auth-port** and **acct-port** parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

Examples To create a RADIUS server group 'RAD_AUTH1' for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000 acct-port
0
```

To create a RADIUS server group 'RAD_ACCT1' for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0 acct-port 1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group 'GROUP1', use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

Related commands [aaa group server](#)
[radius-server host](#)

show debugging radius

Overview This command displays the current debugging status for the RADIUS servers.

Syntax show debugging radius

Mode User Exec and Privileged Exec

Example To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

Output The following shows typical output.

Example output from the show debugging radius command

```
RADIUS debugging status:  
RADIUS event debugging is off  
RADIUS packet debugging is off
```

show radius

Overview This command displays the current RADIUS server configuration and status.

Syntax show radius

Mode User Exec and Privileged Exec

Example To display the current status of RADIUS servers, use the command:
awplus# show radius

Output The following shows typical output.

Example output from the show radius command showing RADIUS servers

```
RADIUS Global Configuration
Source Interface : not configured
Secret Key : secret
Timeout : 5 sec
Retransmit Count : 3
Deadtime : 20 min
Server Host : 192.168.1.10
Authentication Port : 1812
Accounting Port : 1813
Secret Key : secret
Timeout : 3 sec
Retransmit Count : 2
Server Host : 192.168.1.11
Authentication Port : 1812
Accounting Port : not configured

Server Name/   Auth   Acct   Auth   Acct
IP Address    Port   Port   Status Status
-----
192.168.1.10  1812   1813   Alive  Alive
192.168.1.11  1812   N/A    Alive  N/A
```

Example See the sample output below showing RADIUS client status and RADIUS configuration:
awplus# show radius

Output The following shows typical output.

Example output from the show radius command showing RADIUS client status

```
RADIUS global interface name: awplus
Secret key:
Timeout: 5
Retransmit count: 3
Deadtime: 0

Server Address: 150.87.18.89
Auth destination port: 1812
Accounting port: 1813
Secret key: swg
Timeout: 5
Retransmit count: 3
Deadtime: 0
```

Output Parameter	Meaning
Source Interface	The interface name or IP address to be used for the source address of all outgoing RADIUS packets.
Secret Key	A shared secret key to a radius server.
Timeout	A time interval in seconds.
Retransmit Count	The number of retry count if a RADIUS server does not response.
Deadtime	A time interval in minutes to mark a RADIUS server as "dead".
Interim-Update	A time interval in minutes to send Interim-Update Accounting report.
Group Deadtime	The deadtime configured for RADIUS servers within a server group.
Server Host	The RADIUS server hostname or IP address.
Authentication Port	The destination UDP port for RADIUS authentication requests.
Accounting Port	The destination UDP port for RADIUS accounting requests.
Auth Status	The status of the authentication port. The status ("dead", "error", or "alive") of the RADIUS authentication server and, if dead, how long it has been dead for.
	Alive The server is alive.
	Error The server is not responding.

Output Parameter	Meaning
	Dead The server is detected as dead and it will not be used for deadtime period. The time displayed in the output shows the server is in dead status for that amount of time.
	Unknown The server is never used or the status is unknown.
Acct Status	The status of the accounting port. The status ("dead", "error", or "alive") of the RADIUS accounting server and, if dead, how long it has been dead for.

show radius local-server auth-mac-promiscuous

Overview Use this command to show the status of the **auth-mac-promiscuous** command.

Syntax show radius local-server auth-mac-promiscuous

Mode User Exec

Usage notes In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

Example To display the status of the **auth-mac-promiscuous** command, use the command:

```
awplus# show radius local-server auth-mac-promiscuous
```

Output The following shows typical output.

Example output from show radius local-server auth-mac-promiscuous

```
awplus#show radius local-server auth-mac-promiscuous
Auth-mac promiscuous mode: Disabled
...
```

Related commands [auth-mac-promiscuous](#)

Command changes Version 5.5.3-2.1: command added

undebbug radius

Overview This command applies the functionality of the **no debug radius** .

25

Local RADIUS Server Commands

- Contents**
- **Introduction** on page 1143
 - **attribute (radsrv-grp)** on page 1144
 - **authentication** on page 1147
 - **client (radsecproxy-srv)** on page 1148
 - **client mutual-authentication** on page 1150
 - **client name-check** on page 1151
 - **client trustpoint** on page 1152
 - **clear radius local-server statistics** on page 1154
 - **copy fdb-radius-users (to file)** on page 1155
 - **copy local-radius-user-db (from file)** on page 1157
 - **copy local-radius-user-db (to file)** on page 1158
 - **crypto pki enroll local (deleted)** on page 1159
 - **crypto pki enroll local local-radius-all-users (deleted)** on page 1160
 - **crypto pki enroll local user (deleted)** on page 1161
 - **crypto pki export local pem (deleted)** on page 1162
 - **crypto pki export local pkcs12 (deleted)** on page 1163
 - **crypto pki trustpoint local (deleted)** on page 1164
 - **debug crypto pki (deleted)** on page 1165
 - **domain-style** on page 1166
 - **egress-vlan-id (radsrv-grp)** on page 1167
 - **egress-vlan-name (radsrv-grp)** on page 1168
 - **group (radsrv)** on page 1169
 - **help radius-attribute** on page 1170
 - **nas** on page 1172
 - **nas message-authenticator (radsrv)** on page 1174
 - **radius-secure-proxy local-server** on page 1176
 - **radius-server local** on page 1177
 - **server auth-port** on page 1178
 - **server enable** on page 1179
 - **server trustpoint (radsrv)** on page 1180
 - **show radius local-server group** on page 1182
 - **show radius local-server nas** on page 1183
 - **show radius local-server statistics** on page 1184
 - **show radius local-server trustpoint** on page 1186
 - **show radius local-server user** on page 1187
 - **user (radsrv)** on page 1189

- **vlan (radsrv-grp)** on page 1192

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the local RADIUS server on the device. For more information, see the **Local RADIUS Server Feature Overview and Configuration Guide**.

attribute (radsrv-grp)

Overview Use this command to define a RADIUS attribute for the local RADIUS server user group.

For a complete list of defined RADIUS attributes and values, see the [Local RADIUS Server Feature Overview and Configuration Guide](#).

When used with the **value** parameter the **attribute** command configures RADIUS attributes to the user group. If the specified attribute is already defined then it is replaced with the new value.

Use the **no** variant of this command to delete an attribute from the local RADIUS server user group.

Syntax attribute [repeated] {<attribute-name>|<attribute-id>} <value>
no attribute {<attribute-name>|<attribute-id>}

Parameter	Description
repeated	This optional parameter allows you to set multiple instances of the same attribute name or attribute ID.
<attribute-name>	RADIUS attribute name for standard attributes or Vendor- Specific attributes (see the Local RADIUS Server Feature Overview and Configuration Guide for tables of attributes).
<attribute-id>	RADIUS attribute numeric identifier for standard attributes.
<value>	RADIUS attribute value.

Default By default, no attributes are configured.

Mode Local RADIUS Server User Group Configuration

Usage notes For the Standard attributes, the attribute may be specified using either the attribute name, or its numeric identifier. For example, the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

In the same way, where the specific attribute has a pre-defined value, the parameter *<value>* may be substituted with the Value Name or with its numeric value, for example the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause  
user-request
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

or the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

You can define more than one instance of an attribute name (or id) by using the **repeated** parameter. For example:

```
awplus(config-radsrv-group)# attribute repeated Nas-filter-Rule  
"deny in tcp from any to 0.0.0.0/0 23"
```

```
awplus(config-radsrv-group)# attribute repeated Nas-filter-Rule  
"deny in tcp from any to fe80::b1 23"
```

Examples To define the attribute name 'Service-Type' with Administrative User (6) to the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type 6
```

To delete the attribute 'Service-Type' from the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# no attribute Service-Type
```

To define multiple values for attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# attribute repeated NAS-Filter-Rule
"deny in tcp from any to 0.0.0.0/0 23"
awplus(config-radsrv-group)# attribute repeated NAS-Filter-Rule
"deny in tcp from any to fe80::b1 23"
```

To delete a specific value from the attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# no attribute NAS-Filter-Rule "deny
in tcp from any to 0.0.0.0/0 23"
```

Related commands [egress-vlan-id \(radsrv-grp\)](#)
[egress-vlan-name \(radsrv-grp\)](#)
[help radius-attribute](#)

Command changes Version 5.5.0-1.1: **repeated** parameter added

authentication

Overview Use this command to enable the specified authentication methods on the local RADIUS server.

Use the **no** variant of this command to disable specified authentication methods on the local RADIUS server.

Syntax authentication {mac|eapmd5|eaptls|peap}
no authentication {mac|eapmd5|eaptls|peap}

Parameter	Description
mac	Enable MAC authentication method.
eapmd5	Enable EAP-MD5 authentication method.
eaptls	Enable EAP-TLS authentication method.
peap	Enable EAP-PEAP authentication method.

Default All authentication methods are enabled by default.

Mode RADIUS Server Configuration

Examples The following commands enable EAP-MD5 authentication methods on the local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# authentication eapmd5
```

The following commands disable EAP-MD5 authentication methods on Local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no authentication eapmd5
```

Related commands [server enable](#)
[show radius local-server statistics](#)

client (radsecproxy-srv)

Overview Use this command to add a RadSec client (for example, a NAS device) to the RadSecProxy local-server application. The application will accept RADIUS requests from all configured clients.

Use the **no** variant of this command to delete a previously-configured client from the RadSecProxy local-server application.

Syntax client {<hostname>|<ip-addr>} [name-check {on|off}]
no client {<hostname>|<ip-addr>}

Parameter	Description
<	Hostname of client.
<ip-addr>	Specify the client IPv4 address, in dotted decimal notation (A.B.C.D).
n	Specify whether or not to enforce certificate name
c	checking for this client. If the parameter is not specified then the global behavior, which defaults to on , is used.
	Enable name checking for this client.
	Disable name checking for this client.

Mode RadSecProxy Local Server Configuration

Usage notes The client may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each client may be configured to use certificate name-checking; if not specified, the global behavior defined by **client name-check** or **no client name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in this command.

NOTE: If mutual authentication is disabled then this parameter has no effect, see the command.

Example To add a client called 'mynas.local' with certificate name checking **off**, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client mynas.local name-check
off
```


Related **client mutual-authentication**
commands **client name-check**
client trustpoint
radius-secure-proxy local-server

client mutual-authentication

Overview This command enables or disables mutual certificate authentication for all RadSecProxy clients. When enabled, the RadSecProxy local-server application will request and validate an X.509 certificate from the client when establishing a connection.

The **no** variant of this command disables mutual certificate validation. The local-server application will still transmit the local server certificate to the client, but will not expect or validate a certificate from the client.

Syntax client mutual-authentication
no client mutual-authentication

Default Mutual authentication is enabled by default.

Mode RadSecProxy Local Server Configuration

Example Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# no client mutual-authentication
```

Related commands [client \(radsecproxy-srv\)](#)
[client name-check](#)
[radius-secure-proxy local-server](#)

Command changes Version 5.4.6-2.1: command added

client name-check

Overview This command sets the global behavior for certificate name-checking for the RadSecProxy localserver application to **on**. This behavior will be used for all clients associated with the application that do not specify a behavior on a per-client basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **client (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

Syntax client name-check
no client name-check

Default Certificate name checking is on by default.

Mode RadSecProxy Local Server Configuration

Example Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# no client name-check
```

Related commands **client (radsecproxy-srv)**
client trustpoint
radius-secure-proxy local-server

client trustpoint

Overview This command adds one or more trustpoints to be used with the RadSecProxy local-server application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax `client trustpoint [<trustpoint-list>]`
`no client trustpoint [<trustpoint-list>]`

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Mode RadSecProxy Local Server Configuration

Usage notes The device certificate associated with the first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If you enter **client trustpoint** without specifying a trustpoint, the trustpoint list will be unchanged.

If you enter **no client trustpoint** without specifying a trustpoint, all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints to the RadSecProxy local-server by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client trustpoint example_1
awplus(config-radsecproxy-srv)# client trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radsecproxy-srv)# client trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy local-server application using the command:

```
awplus(config-radsecproxy-srv)# no client trustpoint
```

Related **client (radsecproxy-srv)**
commands **client name-check**
radius-secure-proxy local-server

clear radius local-server statistics

Overview Use this command to clear the statistics stored on the device for the local RADIUS server.

Use this command without any parameters to clear all types of local RADIUS server statistics.

Syntax `clear radius local-server statistics [nas|server|user]`

Parameter	Description
nas	Clear the NAS (Network Access Server) statistics on the device. For example, clearing statistics stored for NAS server invalid passwords.
server	Clear the Local RADIUS Server statistics on the device. For example, clearing Local RADIUS Servers statistics for all failed login attempts.
user	Clear the Local RADIUS Server user statistics. For example, clearing statistics stored for the number of successful user logins.

Mode Privileged Exec

Usage Refer to the sample output for the [show radius local-server statistics](#) for further information about the type of statistics each parameter option for this command clears. Both the **nas** and **server** parameters clear unknown username and invalid passwords statistics, while the user parameter clears the number of successful and failed logins for each local RADIUS server user.

Examples To clear the NAS (Network Access Server) statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics nas
```

To clear the local RADIUS server statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics server
```

To clear the local RADIUS server user statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics user
```

Related commands [show radius local-server statistics](#)

copy fdb-radius-users (to file)

Overview Use this command to create a set of local RADIUS server users from MAC addresses in the local FDB. A local RADIUS server user created using this command can be used for MAC authentication.

Syntax `copy fdb-radius-users {local-radius-user-db|nvs|flash|debug|tftp|scp|fserver|<url>} [interface <port>] [vlan <vid>] [group <name>] [export-vlan [<radius-group-name>]]`

Parameter	Description
local-radius-user-db	Copy the local RADIUS server users created to the local RADIUS server.
nvs	Copy the local RADIUS server users created to NVS memory.
flash	Copy the local RADIUS server users created to Flash memory.
debug	Copy the local RADIUS server users created to debug.
tftp	Copy the local RADIUS server users created to the TFTP destination.
scp	Copy the local RADIUS server users created to the SCP destination.
fserver	Copy the local RADIUS server users created to the remote file server.
<url>	Copy the local RADIUS server users created to the specified URL.
interface <port>	Copy only MAC addresses learned on a specified device port. Wildcards may be used when specifying an interface name.
vlan <vid>	Copy only MAC addresses learned on a specified VLAN.
group <name>	Assign a group name to the local RADIUS server users created.
export-vlan	Export VLAN ID assigned to exported FDB entry.
<radius-group-name>	Prefix for Radius group name storing VLAN ID

Mode Privileged Exec

Usage notes The local RADIUS server users created are written to a specified destination file in local RADIUS user CSV (Comma Separated Values) format. The local RADIUS server users can then be imported to a local RADIUS server using the **copy local-radius-user-db (from file)** command.

The name and password of the local RADIUS server users created use a MAC address, which can be used for MAC authentication.

This command does not copy a MAC address learned by the CPU or the management port.

This command can filter FDB entries by the interface name and the VLAN ID. When the interface name and the VLAN ID are specified, this command generates local RADIUS server users from only the MAC address learned on the specified interface and on the specified VLAN.

Examples To register the local RADIUS server users from the local FDB directly to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db
```

To register the local RADIUS server users from the interface port1.0.1 to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db interface  
port1.0.1
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to the file radius-user.csv, use the command:

```
awplus# copy fdb-radius-users radius-user.csv interface  
port1.0.1 vlan10
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to a file on the remote file server, use the command:

```
awplus# copy fdb-radius-users fserver interface port1.0.1 vlan10
```

Related commands **copy local-radius-user-db (to file)**
copy local-radius-user-db (from file)

copy local-radius-user-db (from file)

Overview Use this command to copy the Local RADIUS server user data from a file. The file, including the RADIUS user data in the file, must be in the CSV (Comma Separated Values) format.

You can select **add** or **replace** as the copy method. The **add** parameter option copies the contents of specified file to the local RADIUS server user database. If the same user exists then the old user is removed before adding a new user. The **replace** parameter option deletes all contents of the local RADIUS server user database before copying the contents of specified file.

Syntax `copy <source-url> local-radius-user-db [add|replace]`

Parameter	Description
<source-url>	URL of the source file.
add	Add file contents to local RADIUS server user database.
replace	Replace current local RADIUS server user database with file contents.

Default When no copy method is specified with this command the **replace** option is applied.

Mode Privileged Exec

Examples To replace the current local RADIUS server user data to the contents of `http://datahost/ user.csv`, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db
```

To add the contents of `http://datahost/user.csv` to the current local RADIUS server user database, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db add
```

Related commands [copy fdb-radius-users \(to file\)](#)
[copy local-radius-user-db \(to file\)](#)

copy local-radius-user-db (to file)

Overview Use this command to copy the local RADIUS server user data to a file. The output file produced is CSV (Comma Separated Values) format.

Syntax `copy local-radius-user-db {nvs|flash|tftp|scp|<destination-url>}`

Parameter	Description
nvs	Copy to NVS memory.
flash	Copy to Flash memory.
tftp	Copy to TFTP destination.
scp	Copy to SCP destination.
<destination-url>	URL of the Destination file.

Mode Privileged Exec

Example Copy the current local RADIUS server user data to `http://datahost/user.csv`.

```
awplus# copy local-radius-user-db http://datahost/user.csv
```

Related commands [copy fdb-radius-users \(to file\)](#)
[copy local-radius-user-db \(from file\)](#)

crypto pki enroll local (deleted)

Overview This command is no longer available. Please use the following command instead:

crypto pki enroll *<trustpoint>*

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki enroll local local-radius-all-users (deleted)

Overview This command is no longer available. Please use the following command instead:

crypto pki enroll *<trustpoint>* local-radius-all-users

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki enroll local user (deleted)

Overview This command is no longer available. Please use the following command instead:

crypto pki enroll *<trustpoint>* user *<username>*

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki export local pem (deleted)

Overview This command is no longer available. Please use the **crypto pki export pem** command instead:

```
crypto pki export <trustpoint> pem [terminal|<url>]
```

Note that "local" is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki export local pkcs12 (deleted)

Overview This command is no longer available. Please use the **crypto pki export pkcs12** command instead:

```
crypto pki export <trustpoint> pkcs12 {ca|server|<username>}  
      <url>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki trustpoint local (deleted)

Overview This command is no longer available. Please use the following command instead:

crypto pki trustpoint *<trustpoint>*

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

debug crypto pki (deleted)

Overview This command is no longer available.

domain-style

Overview Use this command to enable a specified domain style on the local RADIUS server. The local RADIUS server decodes the domain portion of a username login string when this command is enabled.

Use the **no** variant of this command to disable the specified domain style on the local RADIUS server.

Syntax domain-style {suffix-atsign|ntdomain}
no domain-style {suffix-atsign|ntdomain}

Parameter	Description
suffix-atsign	Enable at sign "@" delimited suffix style, i.e. "user@domain".
ntdomain	Enable NT domain style, i.e. "domain\user".

Default This feature is disabled by default.

Mode RADIUS Server Configuration

Usage notes When both domain styles are enabled, the first domain style configured has the highest priority. A username login string is matched against the first domain style enabled. Then, if the username login string is not decoded, it is matched against the second domain style enabled.

Examples To enable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# domain-style ntdomain
```

To disable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no domain-style ntdomain
```

Related commands [server enable](#)

egress-vlan-id (radsrv-grp)

Overview Use this command to configure the standard RADIUS attribute 'Egress-VLANID (56)' for the local RADIUS Server user group.

Use the **no** variant of this command to remove the Egress-VLANID attribute from the local RADIUS server user group.

Syntax egress-vlan-id <vid> [tagged|untagged]
no egress-vlan-id

Parameter	Description
<vid>	The VLAN identifier to be used for the Egress VLANID attribute, in the range 1 to 4094.
tagged	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
untagged	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLANID attributes are configured.

Mode Local RADIUS Server User Group Configuration

Examples To set the 'Egress-VLANID' attribute for the 'NormalUsers' local RADIUS server user group to VLAN identifier 200, with tagged frames, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-id 200 tagged
```

To remove the 'Egress-VLANID' attribute for the 'NormalUsers' local RADIUS server user group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-id
```

Related commands [attribute \(radsrv-grp\)](#)
[egress-vlan-name \(radsrv-grp\)](#)

egress-vlan-name (radsrv-grp)

Overview Use this command to configure the standard RADIUS attribute 'Egress-VLAN-Name (58)' for the local RADIUS server user group.

Use the **no** variant of this command to remove the Egress-VLAN-Name attribute from the local RADIUS server user group.

Syntax egress-vlan-name <vlan-name> [tagged|untagged]
no egress-vlan-name

Parameter	Description
<vlan-name>	The VLAN name to be configured as the Egress-VLAN-Name attribute.
tagged	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
untagged	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLAN-Name attributes are configured.

Mode Local RADIUS Server User Group Configuration

Examples To configure the 'Egress-VLAN-Name' attribute for the RADIUS server user group 'NormalUsers' with the VLAN name vlan2 and all frames on this VLAN tagged, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-name vlan2 tagged
```

To delete the 'Egress-VLAN-Name' attribute for the 'NormalUsers' group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-name
```

Related commands [attribute \(radsrv-grp\)](#)
[egress-vlan-id \(radsrv-grp\)](#)

group (radsrv)

Overview Use this command to create a local RADIUS server user group, and enter local RADIUS Server User Group Configuration mode.

Use the **no** variant of this command to delete the local RADIUS server user group.

Syntax group <user-group-name>
no group <user-group-name>

Parameter	Description
<user-group-name>	User group name string.

Mode RADIUS Server Configuration

Examples The following command creates the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
```

The following command deletes the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no group NormalUsers
```

Related commands [user \(radsrv\)](#)
[show radius local-server user](#)
[vlan \(radsrv-grp\)](#)

help radius-attribute

Overview Use this command to display a list of standard and vendor specific valid RADIUS attributes that are supported by the local RADIUS server.

Syntax help radius-attribute [<attribute-name>|<attribute-ID>]

Parameter	Description
<attribute-name>	List the details and predefined values for the named attribute.
<attribute-ID>	List the details and predefined values for the given attribute ID.

Mode Privileged Exec

Usage notes When used without a parameter, this command lists all of the available RADIUS attributes.

When used with an attribute name or ID, this command displays the attribute name, value type, and any predefined values.

Example To list all available RADIUS attributes, use the following command:

```
awplus# help radius-attribute
```

```
awplus#help radius-attribute
Standard Attributes:
 1      User-Name
 2      User-Password
 3      CHAP-Password
 4      NAS-IP-Address
 5      NAS-Port
 6      Service-Type
...
```

To display the details for the RADIUS attribute Frag-Status, use the following command:

```
awplus# help radius-attribute frag-status
```

```
awplus#help radius-attribute frag-status
Frag-Status : integer (Integer number)

Pre-defined values :
  Fragmentation-Supported (1)
  More-Data-Pending (2)
  More-Data-Request (3)
  Reserved (0)
```

Related commands [attribute \(radsrv-grp\)](#)

Command Version 5.4.8-0.2: command added
changes Version 5.4.9-0.1: added to x530 Series products

nas

Overview This command adds a client device (the Network Access Server or the NAS) to the list of devices that are able to send authentication requests to the local RADIUS server. The NAS is identified by its IP address and a shared secret (also referred to as a shared key) must be defined that the NAS will use to establish its identity.

Use the **no** variant of this command to remove a NAS client from the list of devices that are allowed to send authentication requests to the local RADIUS server.

Syntax `nas <ip-address> key <nas-keystring> [encrypted]`
`no nas <ip-address>`

Parameter	Description
<ip-address>	RADIUS NAS IP address.
<nas-keystring>	NAS shared keystring.
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.

Mode RADIUS Server Configuration

Examples The following commands add the NAS with an IP address of 192.168.1.2 to the list of clients that may send authentication requests to the local RADIUS server. Note the shared key that this NAS will use to establish its identity is NAS_PASSWORD.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 192.168.1.2 key NAS_PASSWORD
```

The following commands remove the NAS with an IP address of 192.168.1.2 from the list of clients that are allowed to send authentication requests to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no nas 192.168.1.2
```

Related commands [nas message-authenticator \(radsrv\)](#)
[show radius local-server nas](#)

Command changes Version 5.5.3-2.1: **encrypted** parameter added

nas message-authenticator (radsvr)

Overview Use this command to decide whether or not to require verification of RADIUS packets for a specific NAS. Verification prevents RADIUS protocol forgery attacks. It is achieved by putting a Message-Authenticator attribute in Access-Requests from the NAS.

Use the **no** variant of this command to return the setting to the default.

Syntax nas <ip-address> message-authenticator {required|optional|auto}
no nas <ip-address> message-authenticator

Parameter	Description
<ip-address>	The IP address of the NAS.
required	Discard Access-Requests that have no Message-Authenticator attribute, or that have an invalid Message-Authenticator attribute.
optional	Allow Access-Requests that have no Message-Authenticator attribute, and discard Access-Requests that have an invalid Message-Authenticator attribute.
auto	Determine the mode based on the content of the first Access-Request received. On the basis of this, the device will produce a log message to tell you which mode you should configure. Only use auto temporarily while you are transitioning an existing network or adding new NAS devices with unknown support for Message-Authenticator.

Default auto

Mode RADIUS Server Configuration

Usage notes If you use both MAC authentication and web authentication to authenticate the same TQ Series access point, make sure you set this to **optional**. Otherwise, web authentication may fail.

This is because if the first packet that the server receives from the client contains a valid Message-Authenticator attribute, then by default all subsequent packets from that client must also contain the same Message-Authenticator attribute. If packets don't contain the attribute, the server drops them. This can cause an issue on TQ series APs, because on these APs, MAC authentication's initial packet contains the attribute, and web authentication's initial packet doesn't. This means that web authentication will fail if MAC authentication has already happened.

Setting this to **optional** allows the server to accept packets from a client when the packets don't have a Message-Authenticator attribute, even if the server has already received a packet from that client that contained a Message-Authenticator attribute. This means both web authentication and MAC authentication will succeed, no matter which happens first.

Examples To require Message-Authenticator attributes in messages from a registered NAS whose IP address is 192.168.1.2, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# nas 192.168.1.2 message-authenticator
required
```

To make Message-Authenticator attributes optional in messages from a registered NAS whose IP address is 192.168.1.9, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# nas 192.168.1.9 message-authenticator
optional
```

To return to the default behavior of **auto** for the NAS whose IP address is 192.168.1.9, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# no nas 192.168.1.9 message-authenticator
```

Related commands [ip radius require-message-authenticator nas](#)
[show radius local-server nas](#)

Command changes Version 5.5.4-2.3: command added

radius-secure-proxy local-server

Overview Use this command to enter the RadSecProxy local-server application configuration mode. This application allows remote RadSec clients to communicate with the local RADIUS server process via a secure (TLS) proxy.

Syntax radius-secure-proxy local-server

Mode Global Configuration Mode

Example To change mode from User Exec mode to the RadSecProxy local-server configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)#
```

Related commands

- client (radsecproxy-srv)**
- client name-check**
- client trustpoint**

radius-server local

Overview Use this command to navigate to the Local RADIUS server configuration mode (config-radsrv) from the Global Configuration mode (config).

Note that the local RADIUS server is not supported in VRF. If VRF is configured, the local RADIUS server is only accessible from the default global VRF domain.

Syntax radius-server local

Mode Global Configuration

Example Local RADIUS Server commands are available from config-radsrv configuration mode. To change mode from User Exec mode to the Local RADIUS Server mode (config-radsrv), use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)#
```

Output

```
awplus(config)#radius-server local
Creating Local CA repository.....OK
Enrolling Local System to local trustpoint..OK
awplus(config-radsrv)#
```

Related commands

- server enable**
- show radius local-server group**
- show radius local-server nas**
- show radius local-server statistics**
- show radius local-server user**

server auth-port

Overview Use this command to change the UDP port number for local RADIUS server authentication.

Use the **no** variant of this command to reset the RADIUS server authentication port back to the default.

Syntax server auth-port <1-65535>
no server auth-port

Parameter	Description
<1-65535>	UDP port number.

Default The default local RADIUS server UDP authentication port number is 1812.

Mode RADIUS Server Configuration

Examples The following commands set the RADIUS server authentication port to 10000.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server auth-port 10000
```

The following commands reset the RADIUS server authentication port back to the default UDP port of 1812.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server auth-port
```

Related commands [server enable](#)
[show radius local-server statistics](#)

server enable

Overview This command enables the local RADIUS server. The local RADIUS server feature is started immediately when this command is issued.

The **no** variant of this command disables local RADIUS server. When this command is issued, the local RADIUS server stops operating.

Note that the local RADIUS server is not supported in VRF. If VRF is configured, the local RADIUS server is only accessible from the default global VRF domain.

Syntax server enable
no server enable

Default The local RADIUS server is disabled by default and must be enabled for use with this command.

Mode RADIUS Server Configuration

Examples To enable the local RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

To disable the local RADIUS server, use the command:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server enable
```

Related commands [server auth-port](#)
[show radius local-server statistics](#)

server trustpoint (radsrv)

Overview Use this command to add one or more trustpoints to the local RADIUS server. You can specify multiple trustpoints on one line, or execute the command more than once to add multiple trustpoints to the local RADIUS server.

Use the **no** variant to remove one or more trustpoints from the local RADIUS server.

Syntax `server trustpoint [<trustpoint-list>]`
`no server trustpoint [<trustpoint-list>]`

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted

Default By default, the local trustpoint is associated with the local RADIUS server.

Mode RADIUS Server Configuration

Usage Notes If you do not specify any trustpoints, the command displays a list of trustpoints but leaves the list unchanged.

If you use the **no server trustpoint** command without specifying any trustpoints, then all trustpoints will be removed from the local RADIUS server.

Example To configure a trustpoint called 'my_trustpoint' on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server trustpoint my_trustpoint
```

You can add multiple trustpoints to the local RADIUS server by executing the **server trustpoint** command multiple times:

```
awplus(config-radsrv)# server trustpoint my_trustpoint1
my_trustpoint2
```

To remove the trustpoint called 'my_trustpoint' from the local RADIUS server, use the command:

```
awplus(config-radsrv)# no server trustpoint my_trustpoint
```

To remove all trustpoints from the local RADIUS server, use the command:

```
awplus(config-radsrv)# no server trustpoint
```


Related commands **show radius local-server trustpoint**
server enable
client trustpoint
server trustpoint

Command changes Version 5.4.1-1.1: command added.

show radius local-server group

Overview Use this command to display information about the local RADIUS server user group.

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

Syntax show radius local-server group [*<user-group-name>*]

Parameter	Description
<i><user-group-name></i>	User group name string.

Mode User Exec and Privileged Exec

Example The following command displays Local RADIUS server user group information.

```
awplus# show radius local-server group
```

Output The following shows typical output.

Example output from the show radius local-server group command

Group-Name	Vlan
-----	-----
NetworkOperators	ManagementNet
NormalUsers	CommonNet

Parameters in the output of the show radius local-server group command

Parameter	Description
Group-Name	Group name.
Vlan	VLAN name assigned to the group.

Related commands [group \(radsrv\)](#)

show radius local-server nas

Overview Use this command to display information about NAS (Network Access Servers) registered to the local RADIUS server.

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

Syntax show radius local-server nas [*<ip-address>*]

Parameter	Description
<i><ip-address></i>	Specify NAS IP address for show output.

Mode User Exec and Privileged Exec

Example The following command displays NAS information.

```
awplus# show radius local-server nas
```

Output The following shows typical output.

Example output from the show radius local-server nas command

NAS-Address	Shared-Key (encrypted)	Message Authenticator
127.0.0.1	dbSQ8ED....	optional

Parameters in the output of the show radius local-server nas command

Parameter	Description
NAS-Address	IP address of NAS.
Shared-Key	Shared key used for RADIUS connection.
Message Authenticator	The message-authenticator mode.

Related commands [nas](#)
[nas message-authenticator \(radsvr\)](#)

show radius local-server statistics

Overview Use this command to display statistics about the local RADIUS server.

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

Syntax show radius local-server statistics

Mode User Exec and Privileged Exec

Usage notes Both unknown usernames and invalid passwords will display as failed logins in the show output.

Example The following command displays local RADIUS server statistics.

```
awplus# show radius local-server statistics
```

Output The following shows typical output.

Example output from the show radius local-server statistics command

```
awplus# show radius local-server statistics
Server status      : Run (administrative status is enable)
Enabled methods    : MAC EAP-MD5 EAP-TLS EAP-PEAP
Available methods  : MAC EAP-MD5 EAP-TLS EAP-PEAP
EAP trustpoints    : local
Promiscuous mode   : Enabled
Successes          :7                               Unknown NAS           :0
Failed Logins      :0                               Invalid packet from NAS:0
Internal Error     :0                               Unknown Error          :0

NAS : 127.0.0.1
Successes          :7                               Shared key mismatch    :0
Failed Logins      :0                               Unknown RADIUS message :0
Unknown EAP message :0                               Unknown EAP auth type  :0
Corrupted packet   :0

Users present in the User Database:
Username                               Successes  Failures  LastInteraction
                                         Local time (+00:00)
00-00-00-00-00-01                       0          0         -
00-00-00-00-00-02                       0          0         -
00-15-65-3f-d9-42                       0          0         -
00-90-0b-45-07-e4                       4          0         09 Jan
2024 00:32:24
tester1                                 2          0         09 Jan
2024 00:31:52
tester2                                 0          0         -
user1                                   0          0         -
user1dynvlan                           0          0         -
user2dynvlan                           0          0         -

Users NOT present in the User Database:
Username                               Successes  Failures  Last Interaction
                                         Local time (+00:00)
00-90-0b-45-07-e2                       1          0         09 Jan 2024 00:31:50
```

Related commands **clear radius local-server statistics**
radius-server local
server enable
server auth-port

show radius local-server trustpoint

Overview Displays the PKI trustpoints associated with the local RADIUS server.

Syntax show radius local-server trustpoint

Mode User Exec

Example To show the local RADIUS server trustpoint(s), use the commands:

```
awplus# show radius local-server trustpoint
```

Output The following shows typical output.

Example output from show radius local-server trustpoint

```
show radius local-server trustpoint
Current PKI trustpoints for RADIUS EAP-TLS:
my_trustpoint
```

Related commands

- [server trustpoint \(radsrv\)](#)
- [radius-server local](#)
- [server enable](#)
- [show radius local-server statistics](#)

Command changes Version 5.4.6-1.1: command added

show radius local-server user

Overview Use this command to display information about the local RADIUS server user.

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

Syntax show radius local-server user [*<user-name>*]
show radius local-server user [*<user-name>*] format csv
show radius local-server user [*<user-name>*] detail

Parameter	Description
<i><user-name></i>	RADIUS user name. If no user name is specified, information for all users is displayed.
format csv	Format output as CSV. This parameter is only available in Privileged Exec mode.
detail	Display detailed information about the user.

Mode User Exec and Privileged Exec

Examples The following command displays Local RADIUS server user information for user Tom.

```
awplus# show radius local-server user Tom
```

Example output from the show radius local-server user command

User-Name	Group	Vlan
-----	-----	-----
Tom	NetworkOperators	ManagementNet

The following command displays all Local RADIUS server information for all users.

```
awplus# show radius local-server user
```

The following command displays Local RADIUS server user information for Tom in CSV format (only available in Privileged Exec mode).

```
awplus# show radius local-server user Tom format csv
```

Example output from the show radius local-server user Tom format csv command

```
true,"NetworkOperators","Tom","abcd",0,2099/01/01,1,"","","ManagementNet"false,3600,false,0,"",false
```

The following command displays detailed Local RADIUS server user information for all users.

```
awplus# show radius local-server user detail
```

Example output from the show radius local-server user detail command

```
awplus# show radius local-server user detail
Total users: 1
Maximum users allowed by license: 3
-----
Username   : Tom
Group      : NetworkOperators
Vlan       : VlanName
```

Parameters in the output from the show radius local-server user command

Parameter	Description
User - Name	User name.
Group	Group name assigned to the user.
Vlan	VLAN name assigned to the user.

Related commands [group \(radsrv\)](#)
[user \(radsrv\)](#)

Command changes Version 5.4.9-0.1: **detail** parameter added

user (radsrv)

Overview Use this command to register a user to the local RADIUS server.

Use the **no** variant of this command to delete a user from the local RADIUS server.

Syntax user <radius-user-name> [encrypted] password <user-password>
[group <user-group>]
no user <radius-user-name>

Parameter	Description
<radius-user-name>	RADIUS user name. See the Usage Notes for details. This can also be a MAC address in the IEEE standard format of HH-HH-HH-HH-HH-HH if you are configuring MAC authentication to use local RADIUS server.
encrypted	Specifies that the password is being entered in its encrypted form, so that it is not further encrypted. When creating a new user, enter the password in plaintext, and do not use the encrypted parameter. Use the encrypted parameter only when referring to a user that has previously been created. For instance, when adding an existing user from another RADIUS server, use the encrypted parameter, and enter the encrypted version of the password that appears in the output of show commands for the user.
<user-password>	User password. This can also be a MAC address in the IEEE standard format of HH-HH-HH-HH-HH-HH if you are configuring MAC authentication to use local RADIUS server.
group	Specify the group for the user.
<user-group>	User group name.

Mode RADIUS Server Configuration

Usage notes The user name can contain alphanumeric ASCII characters, plus signs (ASCII 43), dashes (ASCII 45), dots (ASCII 46), @ signs (ASCII 64), slashes (ASCII 47), backslashes (ASCII 92), and underscores (ASCII 95). It cannot contain spaces. It must not start with a digit, a plus sign, a dash or an @ sign. It must not end with an @ sign. On the AlliedWare Plus CLI, it is case sensitive.

It cannot contain question marks (?), spaces (), or double quote characters.

RADIUS user names containing the following characters cannot use certificate authentication:

/ \ \$ & () * ; < > |

Certificates cannot be created and exported for RADIUS user names that contain the above characters. We advise you to avoid using these characters in RADIUS user names if you need to use certificate authentication, because you will not be able to create and export certificates.

You also can use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) to specify a supplicant MAC address to configure the user name and user password parameters to use local RADIUS server for MAC Authentication. See the [AAA and Port_Authentication Feature Overview and Configuration_Guide](#) for a sample MAC configuration. See also the command **user 00-db-59-ab-70-37 password 00-db-59-ab-70-37** as shown in the command examples.

Examples The following commands add user 'Tom' to the local RADIUS server and sets his password to 'QwerSD'.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD
```

The following commands add user 'Tom' to the local RADIUS server user group 'NormalUsers' and sets his password 'QwerSD'.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD group
NormalUsers
```

The following commands remove user 'Tom' from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user Tom
```

The following commands add the supplicant MAC address 00-d0-59-ab-70-37 to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user 00-db-59-ab-70-37 password 00-db-59-
ab-70-37
```

The following commands remove the supplicant MAC address 00-d0-59-ab-70-37 from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user 00-db-59-ab-70-37
```

Related commands [group \(radsrv\)](#)
[show radius local-server user](#)

vlan (radsrv-grp)

Overview Use this command to set the VLAN ID or name for the local RADIUS server user group. The VLAN information is used for authentication with the dynamic VLAN feature.

Use the **no** variant of this command to clear the VLAN ID or VLAN name for the local RADIUS server user group.

Syntax `vlan {<vid>|<vlan-name>}`
`no vlan`

Parameter	Description
<vid>	VLAN ID.
<vlan-name>	VLAN name.

Default VLAN information is not set by default.

Mode Local RADIUS Server User Group Configuration

Examples The following commands set VLAN ID 200 to the group named 'NormalUsers':

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# vlan 200
```

The following commands remove VLAN ID 200 from the group named 'NormalUsers':

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no vlan
```

Related commands [group \(radsrv\)](#)
[show radius local-server user](#)

26 Two-factor Authentication (2FA) Commands

- Contents**
- **Introduction** on page 1194
 - **2fa allow-reuse** on page 1195
 - **2fa create user** on page 1196
 - **2fa create user email** on page 1198
 - **2fa create user skip-2fa** on page 1199
 - **2fa delete user** on page 1200
 - **2fa email-expiry-time** on page 1201
 - **2fa email-otp** on page 1202
 - **2fa email-template** on page 1203
 - **2fa export user-data** on page 1205
 - **2fa hotp-window-size** on page 1206
 - **2fa import user-data source** on page 1208
 - **2fa issuer** on page 1210
 - **2fa label** on page 1212
 - **2fa max-skew** on page 1214
 - **2fa radius-email-attribute** on page 1216
 - **2fa reject-unconfigured-users** on page 1218
 - **2fa reset scratch-codes** on page 1219
 - **2fa reset skew** on page 1220
 - **2fa skew adjust** on page 1221
 - **2fa totp-window-size** on page 1223
 - **2fa self-registration port** on page 1225
 - **aaa authentication 2fa-registration default group** on page 1227
 - **debug 2fa** on page 1229
 - **email-attribute (ldap-server)** on page 1230
 - **service 2fa** on page 1231
 - **show 2fa** on page 1233
 - **show 2fa email-template** on page 1234
 - **show 2fa user** on page 1235
 - **show 2fa users** on page 1237
 - **show debugging 2fa** on page 1238
 - **undebug 2fa** on page 1239

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure two-factor authentication (2FA).

2FA is a method of strengthening security by requiring a second method of authentication. AlliedWare Plus supports 2FA on OpenVPN connections. It requires a software-based authenticator that implements either the time-based one-time password (TOTP) or the HMAC-based one-time password (HOTP) algorithms. These software authenticators (known as authenticator apps) are usually loaded on a mobile device. One well-known implementation of such an app is Google Authenticator.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

2fa allow-reuse

Overview Use this command, when configuring two-factor authentication (2FA), to allow the reuse of time-based codes within the acceptable time window. By default, if a code has already been used then it will be rejected. This means the user must wait for the next code to appear in their authenticator app to be able to login.

Use the **no** variant of this command to return to the default state, which is to reject codes that have already been used.

Syntax 2fa allow-reuse
no 2fa allow-reuse

Default Disabled

Mode Global Configuration

Usage notes The 2FA service must be running for this command to work. Enable it with the **service 2fa** command.

Example To allow the reuse of time-based codes, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa allow-reuse
```

To prevent the reuse of time-based codes, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa allow-reuse
```

Related commands

- 2fa create user**
- 2fa delete user**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa create user

Overview Use this command to create the two-factor authentication (2FA) data for a user. It allows you to set the authentication mode, HMAC-based One-Time Password (HOTP) or Time-based one-time password (TOTP), and displays a QR code and scratch codes for the user.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

Syntax `2fa create user <user-name> {random-secret|secret <secret-key>} [hotp] [qr {ansi|utf8|link}]`

Parameter	Description
<user-name>	The name of the user you are creating.
random-secret	Generate a random secret key.
secret	Use a pre-defined secret key.
<secret-key>	The pre-defined secret key.
hotp	Use HOTP mode for code verification (the default is TOTP).
qr	Display the QR code
ansi	Display the QR code using ANSI block characters.
utf8	Display the QR code using a UTF-8 mosaic.
link	Display a hyperlink for a QR code generator. Opening the link in a browser will display a QR code. As the string is passed to an online QR code generator (at Google), it may be a security concern for some installations.

Mode Privileged Exec

Usage notes You must enable the 2FA service, with the [service 2fa](#) command, before creating user data.

The QR code displays best in a color mode ANSI or UTF-8 terminal. If your terminal is insufficiently wide, or doesn't have the correct options enabled, you may not get a scannable QR code.

Example To create a user 'test', generate a random secret key, use HOTP mode, and display a QR link, use the command:

```
awplus# 2fa create user test random-secret hotp qr link
```


Output The following shows typical output.

Example output from 2fa create user test random-secret hotp qr link

```
awplus#2fa create user test random-secret hotp qr link
Two-Factor Authentication information for user:

Username:      test
Secret:        IWNZKQS2WXQ6I2VHGTUFP4IVA4
Mode:          HOTP (counter: 1)
OTP            URL:otpath://hotp/test@awplus?secret=IWNZKQS2WXQ6I2VHGTUFP4IVA4
Scratch codes:
59808697
25389232
71366922
48035778
82664010

The following URL can be used to generate a QR code.
This results in the user key being sent to Google servers.
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpath://hotp/
test@awplus%3Fsecret%3DIWNZKQS2WXQ6I2VHGTUFP4IVA4awplus#
```

Related commands

- 2fa delete user**
- 2fa reset skew**
- 2fa reset scratch-codes**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa create user email

Overview Use this command to create a Two-Factor Authentication (2FA) email user entry. This allows users authenticating through OpenVPN to use the 2FA email One-Time-Password feature (2FA email OTP).

Syntax `2fa create user <user-name> email <email-address>`

Parameter	Description
<code><user-name></code>	User name, for example, 'test1'
<code><email-address></code>	User email address, for example, 'test1@xyz.com'

Default No user email is created.

Mode Privileged Exec

Usage notes 2FA users can be emailed their OTP instead of using their mobile device app to generate their OTP.

Example To configure the user 'test1' with the email address 'test1@xyz.com', use the command:

```
awplus# c2fa create user test1 email test1@xyz.com
```

Related commands

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [2fa create user skip-2fa](#)

Command changes Version 5.5.3-0.1: command added

2fa create user skip-2fa

Overview Use this command to create a Two-Factor Authentication skip-2fa user entry. This enables users authenticating through OpenVPN to skip 2FA requirements.

This means that these users do not need to generate One-Time-Passwords (OTP) from a time-based OTP authenticator app or email OTP code.

Syntax 2fa create user <user-name> skip-2fa

Parameter	Description
<user-name>	The name of the user, for example, 'Test1'

Default No 2FA skip-2fa user entry exists.

Mode Privileged Exec

Usage notes To remove a 2FA skip-2fa user entry, use the command **2fa delete user**.

Example To create a user named 'Test1' that can skip the 2FA requirements, use the command:

```
awplus# 2fa create user Test1 skip-2fa
```

Related commands [2fa create user](#)
[2fa delete user](#)
[2fa create user email](#)

Command changes Version 5.5.3-0.1: command added

2fa delete user

Overview Use this command to delete the two-factor authentication (2FA) data for a user.

Syntax 2fa delete user <user-name>

Parameter	Description
<user-name>	The name of the user you are deleting.

Mode Privileged Exec

Example To delete the 2FA data for a user named 'test', use the command:

```
awplus# 2fa delete user test
```

Related commands

- [2fa create user](#)
- [2fa reset scratch-codes](#)
- [2fa reset skew](#)
- [service 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

Command changes Version 5.5.2-1.1: command added

2fa email-expiry-time

Overview A Two-Factor Authentication (2FA) user email code will be valid only for a certain time after it is generated. The default time period is 10 minutes. This command sets an expiry time globally.

Use the **no** variant of this command to reset the expiry time back to the default (10 minutes).

Syntax 2fa email-expiry-time <1-1440>
no 2fa email-expiry-time

Parameter	Description
<1-1440>	The expiry time in minutes, for example, 20 minutes.

Default 10 minutes

Mode Global Configuration

Examples To set 2FA user email OTP expiry time to 20 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa email-expiry-time 20
```

To reset 2FA user email OTP expiry time back to the default (10 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa email-expiry-time
```

Related commands [2fa email-otp](#)
[2fa email-template](#)
[service 2fa](#)

Command changes Version 5.5.3-01: command added

2fa email-otp

Overview Use this command to enable the Two-Factor Authentication email One-Time-Password (OTP) feature. The 2FA email OTP feature emails the password instead of receiving it with an authenticating mobile app. The emailed OTP allows you to connect to an OpenVPN tunnel.

Use the **no** variant of this command to disable the 2FA email OTP feature.

Syntax 2fa email-otp
no 2fa email-otp

Default Disabled

Mode Global Configuration

Examples To enable the 2FA email OTP feature, use the commands:

```
awplus# configure terminal  
awplus(config)# 2fa email-otp
```

To disable the 2FA email OTP feature, use the commands:

```
awplus# configure terminal  
awplus(config)# no 2fa email-otp
```

Output The following shows typical output.

Example output from 2fa email-otp

```
Sub-feature 2FA email OTP is enabled
```

Related commands [service 2fa](#)

Command changes Version 5.5.3-0.1: command added

2fa email-template

Overview Use this command to set the location of the Two-Factor Authentication email One-Time-Password (2FA email OTP) template file.

Use the **no** variant of this command to set the email template file back to the default.

Syntax 2fa email-template <file-name>
no 2fa email-template>

Parameter	Description
<file-name>	The name of the email template file saved to flash memory on your device, for example 'email_template.txt'.

Default Default email template file contents

	Subject: %%LABEL%% 2FA Email OTP code
	Verification code: %%OTP%%
	The verification code will expire in %
	%EXPIRY_TIME%% minutes.
	This is an automated message, please do not
	reply.

Mode Global Configuration

Usage notes A subject line with an empty line immediately following it is required. There are some words surrounded by %% signs. These are replaced by the specified details when the email is sent. There are five different options for these, each of which can be used multiple times if needed:

Parameter options for the email template

Template Parameter	Description
%%OTP%%	The OTP code that the user can use to log in. This must be included in the template.
%%USERNAME%%	The username of the user who is attempting to connect.
%%EMAIL_ADDR% %	The email address of the user, which the email will be sent to.
%%EXPIRY_TIME% %	The number of minutes that the OTP will be valid for.
%%LABEL%%	A configurable label that is set by the 2FA configuration, which is also displayed in application-based 2FA.

Example To configure an email template, first the new email template needs to be saved to a file on the flash memory of your device. For example:

Example email template file named email_template.txt

```
Subject: %%LABEL%% 2FA Email OTP code for %%USERNAME%%  
  
Verification code: %%OTP%%  
  
The verification code will expire in %%EXPIRY_TIME%% minutes.  
This is an automated message, please do not reply.  
  
This email was intended for %%EMAIL_ADDRESS%%.  
Send by %%LABEL%%
```

To configure the template file named 'email_template.txt', use the commands:

```
awplus# configure terminal  
awplus(config)# 2fa email-template email_template.txt
```

Related commands

- [2fa label](#)
- [2fa email-otp](#)
- [2fa email-expiry-time](#)
- [show 2fa email-template](#)

Command changes Version 5.5.3-0.1: command added

2fa export user-data

Overview Use this command to export Two-Factor Authentication (2FA) user data to a flash file.

Syntax 2fa export user-data

Default No files are exported

Mode Privileged Exec

Usage notes 2FA user data will be exported to a local flash file only. The data will be compressed and encrypted with a password. An administrator transports the flash file and copies it to a location where it can then be copied to another AlliedWare plus device for importation.

Use the command **2fa import user-data source** to import the user data after exporting it with this command.

Example To export 2FA user data to a flash file, use the command:

```
awplus# 2fa export user-data
```

Output The following shows typical output.

Example output from 2fa export user-data

```
awplus#2fa export user-data
Enter security password:
Re-enter password:
Successfully exported 2FA user data (11 users) to file
  atl2fausers-20230303-3272.dat
awplus#
```

Related commands [2fa import user-data source](#)

Command changes Version 5.5.3-0.1: command added

2fa hotp-window-size

Overview Use this command to set the range of acceptable codes for HMAC-based one-time password (HOTP) mode two-factor authentication (2FA). The window size is the number of codes checked, starting at the current stored counter value, and then checking forward.

Use the **no** variant of this command to reset the window size to the default of 3.

Syntax 2fa hotp-window-size <1-100>
no 2fa hotp-window-size

Parameter	Description
<1-100>	The number of codes valid from the current counter value.

Default 3

Mode Global Configuration

Usage notes The stored counter value is the counter value after the last successfully verified code. If a code later in the window is detected, the stored counter is updated to that value. This helps keep the mobile authenticator app and device synchronized. For example, the default HOTP window size of 3 allows the device to accept the current code or the following 2 codes.

Example To set the window size to include codes for the current and next 4 counter values (a total of 5 codes), use the commands:

```
awplus# configure terminal
awplus(config)# 2fa hotp-window-size 5
```

To set the window size to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa hotp-window-size
```

Related commands

- 2fa create user**
- 2fa delete user**
- 2fa totp-window-size**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa import user-data source

Overview Use this command to import Two-Factor Authentication (2FA) user data when you want to load the data to a different AlliedWare Plus device.

Syntax `2fa import user-data source <file-location> [replace]`

Parameter	Description
<file-location>	The file location containing the user data.
replace	Indicate whether to replace existing user data.

Default No user file is imported

Mode Privileged Exec

Usage notes To import user data, the 2FA service must be stopped. Use the **no** variant of the command [service 2fa](#).

Currently, the user information is stored in `flash:/.configs/.atl_2fa_users`. If this file is copied to a new device before the 2FA service is started, the 2FA service will load the users at startup. This file is backed up and restored with AMF backup.

An administrator can use this command to transport the flash file and copy it to a safe location. This file can then be imported to another AlliedWare Plus device. The user data will be decompressed and decrypted with the same user password that it was exported with.

The imported user data can either replace or merge with existing 2FA user data.

Example In this example, the user data file is merged with any existing user data.

To import the user data file 'tftp://192.168.1.1/atl2fausers-20230303-3321.dat', use the commands:

```
awplus# c2fa import user-data source tftp://192.168.1.1/  
atl2fausers-20340303-3321.dat  
awplus(config)# command name
```

Output The following shows typical output.

Example output from 2fa import user-data source

```
awplus#2fa import user-data source tftp://192.168.1.1/  
atl2fausers-20230303-3321.dat  
Copying...  
Successful operation  
Enter security password:  
Successfully imported 2FA user data (11 users).  
awplus#
```

Related commands [2fa export user-data](#)
[service 2fa](#)

Command changes Version 5.5.3-0.1: command added

2fa issuer

Overview Use this command to set an optional issuer string that is used in the two-factor authentication (2FA) QR code. The issuer string will then be set in every user's QR code.

By default, the issuer string is not set.

Use the **no** variant of this command to set the issuer string to be empty.

Syntax 2fa issuer <issuer-name>
no 2fa issuer

Parameter	Description
<issuer-name>	Text string to include in the OTP URL in the issuer field.

Default Issuer not set

Mode Global Configuration

Usage notes The Quick Response (QR) code is built from the OTP URL. The QR code can be used to load the shared secret into an authenticator app. The label and issuer strings affect how the entry is displayed in the authenticator app.

For example, in the URL below the issuer has been set to 'ATL':

OTP URL:	otpauth://totp/test@awplus?secret=RIVS3...&issuer=ATL

Once the issuer has been changed it is possible to display a QR code for existing users, with the new issuer included, by using the **show 2fa user** command.

The 2FA service must be running for this command to work.

Example To set the issuer to 'ATL', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa issuer ATL
```

Related commands

- 2fa create user**
- 2fa delete user**
- 2fa label**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa label

Overview Use this command to set an optional label string that is used in the two-factor authentication (2FA) QR code. The label string will be set in every user's QR code.

By default the label is the system's host name.

Use the **no** variant of this command to set the label field back to the host name.

Syntax `2fa label <label-string>`
`no 2fa label`

Parameter	Description
<code><label-string></code>	Text string to include in the OTP URL in the label field.

Default System's host name

Mode Global Configuration

Usage notes The Quick Response (QR) code is built from the OTP URL. The QR code can be used to load the shared secret into an authenticator app. The label and issuer strings affect how the entry is displayed in the authenticator app.

The full label that AlliedWare Plus produces is `<username>@<label>`. For example, in the URL below the default host name is being used with user name 'test':

```
OTP URL:  otpauth://totp/test@awplus?secret=RIVS3...&issuer=ATL
```

Once the label has been changed it is possible to display a QR code for existing users, with the new label included, by using the [show 2fa user](#) command.

The 2FA service must be running for this command to work.

Example To set the label to 'Company VPN', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa label Company VPN
```


Related commands

- 2fa create user**
- 2fa delete user**
- 2fa issuer**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa max-skew

Overview Use this command to set the maximum time skew to be used by the time skew adjustment feature. The time skew adjustment feature is enabled with the **2fa skew adjust** command.

By default, 1500 extra codes are checked in each direction from the current time-step. This is 12.5 hours maximum skew in either direction (codes are generated in 30 second time-step intervals).

Use the **no** variant of this command to reset the maximum number of time-steps to check to 1500.

Syntax 2fa max-skew <120-3000>
no 2fa max-skew

Parameter	Description
<120-3000>	Maximum number of 30 second time-steps to check.

Default 1500

Mode Global Configuration

Example To configure the time skew adjustment feature to check a maximum of one hour (i.e. 120 30 second time-steps), either side of the current time-step, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa max-skew 120
```

To configure the time skew adjustment feature to check a maximum of 25 hours (i.e. 3000 30 second time-steps), either side of the current time-step, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa max-skew 3000
```

Related commands

- 2fa reset skew**
- 2fa skew adjust**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa radius-email-attribute

Overview Use this command to set the RADIUS attributes to transfer the user email address or domain to the server for Two-Factor Authentication.

These attributes are used for 2FA email One-Time-Password (OTP) to send the password to the user.

Use the **no** variant of this command to remove the RADIUS attributes from the server.

Syntax 2fa radius-email-attribute {email <email-address>|domain <domain-name>}
no 2fa radius-email-attribute

Parameter	Description
<email-address>	Email address, for example, 'User-Name'
<domain-name>	Domain name, for example, 'Framed-Pool'

Default No RADIUS attribute is set for user email address or domain.

Mode Global Configuration

Usage notes The RADIUS attribute for the email or domain must be an ASCII text string attribute. This can be checked by using the **help** command in AlliedWare Plus to check whether the type of an attribute is a string.

The RADIUS server can either be retrieved completely from a RADIUS attribute, or constructed using the user's username combined with the value of a RADIUS attribute containing a domain name. For example, <username>@<domain-name>.

Example output from the help command

```
awplus#help radius-attribute
Standard Attributes:
 1 User-Name
 2 User-Password
 3 CHAP-Password
 4 NAS-IP-Address
...
awplus#help radius-attribute framed-pool
Framed-Pool : string (Character string)
```

Examples To use the RADIUS attribute 'User-Name' to transfer a user's email address to the server, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# 2fa radius-email-attribute email User-Name
```

To use the RADIUS attribute 'Framed-Pool' to transfer a user's domain to the server, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# 2fa radius-email-attribute domain Framed-Pool
```

To reset the RADIUS attribute back to the default, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no 2fa radius-email-attribute
```

Output The following shows typical output.

Example output from 2fa radius-email-attribute

```
The selected Radius attributes will be used to convey user email  
address or domain.
```

Related commands [2fa email-otp](#)
[email-attribute \(ldap-server\)](#)

Command changes Version 5.5.3-0.1: command added

2fa reject-unconfigured-users

Overview Use this command to deny authentication to users who have not been configured for two-factor authentication (2FA). By default, if a user is not configured for 2FA then 2FA will be skipped during the authentication process.

Use the **no** variant of this command to allow users to authenticate even if they are not configured for 2FA.

Syntax 2fa reject-unconfigured-users
no 2fa reject-unconfigured-users

Default Users not configured for 2FA are allowed to authenticate.

Mode Global Configuration

Example To deny authentication to users who don't have 2FA configured, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa reject-unconfigured-users
```

Related commands

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

Command changes Version 5.5.2-1.1: command added

2fa reset scratch-codes

Overview Use this command to generate a set of five new scratch codes for a two-factor authentication (2FA) user. Each scratch code can only be used once.

Syntax `2fa reset scratch-codes user <user-name>`

Parameter	Description
user	Reset scratch codes for a user.
<user-name>	Name of the user you want to generate scratch codes for.

Mode Privileged Exec

Usage notes When a 2FA user is created, 5 scratch codes are created for that user. These are one time emergency codes that can be used in place of a code generated by the authenticator app. Once they are used, they can not be used again. Use this command to generate 5 new scratch codes for a user.

Example To reset the 2FA scratch codes for the user named 'test', use the command:

```
awplus# 2fa reset scratch-codes user test
```

Output The following shows typical output.

Example output from `2fa reset scratch-codes user test`

```
Scratch codes:
70344616
91312817
39931705
89513481
78647666
```

Related commands

- [2fa create user](#)
- [2fa delete user](#)
- [2fa reset skew](#)
- [show 2fa user](#)
- [show 2fa users](#)

Command changes Version 5.5.2-1.1: command added

2fa reset skew

Overview Use this command to reset the skew adjustment data for a two-factor authentication (2FA) user. Time skew adjustment data is recorded for a user if the time skew adjustment feature is enabled with the **2fa skew adjust** command.

Syntax 2fa reset skew user <user-name>

Parameter	Description
user	Reset for a user.
<user-name>	The name of the user you want to reset.

Mode Privileged Exec

Example To reset the skew data for a user called 'test', use the command:

```
awplus# 2fa reset skew user test
```

Related commands

- 2fa max-skew**
- 2fa skew adjust**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa skew adjust

Overview Use this command to enable the time skew adjustment feature for time-based one-time password (TOTP) two-factor authentication (2FA).

TOTP authentication depends on the clock on the authenticating device and the clock on the authenticator app being synchronized. If there is a difference in time larger than what is covered by the TOTP window size then the client will not be able to authenticate. Time skew adjustment provides a method to detect and store this time difference and allow them to authenticate if it is consistent.

Use the **no** variant of this command to disable the time skew adjustment feature.

Syntax 2fa skew-adjust
no 2fa skew-adjust

Default Time skew adjustment is disabled.

Mode Global Configuration

Usage notes The most likely cause of time skew (other than the clock being set wrong on the authenticator or authenticating device) is an incorrectly configured timezone.

When time skew adjustment is enabled, extra checking happens after an incorrect login. When an incorrect login occurs, the device will check a large number of codes either side of the current time. If it finds one that matches, it will record the **skew** of the code.

If the user enters 3 incorrect (but different) codes the device checks:

- were these codes entered in quick succession, i.e. with no more than one time-step gap between them, and
- did they all have the same skew value?

If these conditions are satisfied then the device will record this as an offset (time skew) and automatically adjust which codes it checks for that user in future.

The maximum number of codes to check is configurable with the **2fa max-skew** command. It defaults to 12.5 hours in either direction.

If a time skew value has been stored for a user this will be displayed (with a warning) in the **show 2fa user** command output.

Example To enable the time skew adjustment feature, use the following commands:

```
awplus# configure terminal
awplus(config)# 2fa skew-adjust
```

Related commands

- 2fa max-skew**
- 2fa reset skew**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa totp-window-size

Overview Use this command to set the range of acceptable codes for time-based one-time password (TOTP) mode two-factor authentication (2FA). The window size is the number of codes checked, centered on the current time-step.

Use the **no** variant of this command to reset the window size to the default of 3.

Syntax 2fa totp-window-size <1-100>
no 2fa totp-window-size

Parameter	Description
<1-100>	The number of codes valid for a given time-step, centered on the current time-step.

Default 3

Mode Global Configuration

Usage notes By default the TOTP window size is set to 3. This means that the code for the current, previous, and next 30 second time-step will be accepted. If the value is set to 1, only the code for the current time-step will be accepted. If it is increased, more time-steps each side of the current time-step will be accepted.

Example To set the window size to include codes for the two previous time-steps, the current, and the two time-steps following the current time (i.e. a total of 5 codes), use the commands:

```
awplus# configure terminal
awplus(config)# 2fa totp-window-size 5
```

To set the window size to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa totp-window-size
```

Related commands

- 2fa create user**
- 2fa delete user**
- 2fa hotp-window-size**
- service 2fa**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

2fa self-registration port

Overview Use this command to enable Two-Factor Authentication (2FA) user self-registration and specify the HTTPS port.

Use the **no** variant of this command to disable 2FA user self-registration.

Syntax 2fa self-registration port <port-number>
no 2fa self-registration

Parameter	Description
<port-number>	The port number from the range 1 to 65535. For example, port 443.

Default Disabled

Mode Global Configuration

Usage notes The 2FA service must be running for this command to work. Use the **service 2fa** command to enable the 2FA service.

The port parameter allows the user to register on a specified port. A user can register by accessing the website hosted on the device at: `https://<device-ip>:<port>/2fa-registration`

The port specified in the command can be set to the same port as the port specified in the command **http secure-port**, or the default secure port if one has not been set. However, it cannot be set to the HTTP port. The HTTP port is 80 by default, unless it has been changed with the command **http port**.

Also, if PAC file hosting is enabled, then the user self-registration port must be set to a different port if it is not the same as the HTTP secure port.

While 2FA user self registration is disabled, the webpage is hidden. If someone tries to browse to it, they will see an error.

Example To enable 2FA user self-registration and specify the HTTPS port '443', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa self-registration port 443
```

To disable 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa self-registration
```

Related commands **service 2fa**

Command changes Version 5.5.3-0.1: command added

aaa authentication 2fa-registration default group

Overview Use this command to set authentication methods for Two-Factor Authentication (2FA) user self-registration.

Use the **no** variant of this command to unset authentication methods for 2FA user self-registration.

Syntax `aaa authentication 2fa-registration default group {ldap|radius|
<group-name>}`
`no aaa authentication 2fa-registration default`

Parameter	Description
ldap	Use all LDAP servers configured by the ldap-server name command.
radius	Use all RADIUS servers configured by the radius-server host command.
<group-name>	The name of the LDAP or RADIUS server group to authenticate self-registration users with.

Default No servers are configured by default

Mode Global Configuration

Examples To configure LDAP servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group ldap
```

To configure RADIUS servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group radius
```

To configure a selected LDAP or RADIUS group of servers called 'GRP1' to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group GRP1
```

To remove the configured server group for 2FA self-registration to authenticate with, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication 2fa-registration default
```

Related commands [2fa self-registration port service 2fa](#)

Command changes Version 5.5.3-0.1: command added

debug 2fa

Overview Use this command to turn on two-factor authentication (2FA) debug messaging.

Use the **no** variant of this command to turn off 2FA debug messaging.

Syntax debug 2fa
no debug 2fa

Default Debug messaging is turned off.

Mode Privileged Exec

Example To turn on 2FA debug messaging, use the command:

```
awplus# debug 2fa
```

Related commands [service 2fa](#)
[show debugging 2fa](#)

Command changes Version 5.5.2-1.1: command added

email-attribute (ldap-server)

Overview Use this command to set the attribute that the LDAP server stores user emails in for the Two-Factor Authentication One Time Password feature (2FA OTP). The attribute is used to retrieve the user email address that the 2FA OTP feature uses to email an OTP to the user.

Use the **no** variant of this command to set the attribute back to the default.

Syntax email-attribute <attribute-name>
no email-attribute

Parameter	Description
<attribute-name>	LDAP mail attribute name. For example, UserCustomData.

Default The default LDAP email attribute is userPrincipalName

Mode LDAP Server Configuration

Examples To set the attribute 'UserCustomData' as the email attribute for the LDAP server 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# email-attribute UserCustomData
```

To reset the attribute back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no email-attribute
```

Output The following shows typical output.

Example output from email-attribute

```
email attribute changed.
```

Related commands [ldap-server](#)
[2fa email-otp](#)

[2fa radius-email-attribute](#)

Command changes Version 5.5.3-0.1: command added

service 2fa

Overview Use this command to enable Two-Factor Authentication (2FA).

2FA is a method of strengthening security by requiring a second method of authentication. AlliedWare Plus supports 2FA on OpenVPN connections. It requires a software-based authenticator that implements the time-based one-time password (TOTP) or HMAC-based one-time password (HOTP) algorithms.

These software authenticators (known as authenticator apps) are usually loaded on a mobile device. Google Authenticator is one well-known implementation of an authenticator app.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

Use the **no** variant of this command to disable 2FA.

Syntax service 2fa
no service 2fa

Default Disabled

Mode Global Configuration

Usage notes Disabling the 2FA service stops the 2FA configuration from showing in the running configuration and prevents 2FA commands from working. You will not be able to view, create, or delete users with the service stopped. User data, however, is not deleted.

Additionally, the 2FA configuration is not reset until the device is rebooted. This means the configuration will be restored if the service is restarted before the device is rebooted.

If the OpenVPN method list is configured with 2FA and the 2FA service is not running, then two-factor authentication will be skipped and a critical message will be logged when a user connects.

Example To enable the 2FA service, use the command:

```
awplus# service 2fa
```

To disable the 2FA service, use the command:

```
awplus# no service 2fa
```

Related commands

- 2fa create user**
- 2fa delete user**
- show 2fa**
- show 2fa user**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

show 2fa

Overview Use this command to display information about your Two-Factor Authentication (2FA) configuration and the status of the 2FA service.

Syntax show 2fa

Mode Privileged Exec

Example To display information on your 2FA configuration and status, use the command:

```
awplus# show 2fa
```

Output The following shows typical output.

Example output from show 2fa

```
awplus#show 2fa

Settings:
  Allow TOTP code reuse:      No
  Reject users with no config: No
  Allow user self-registration: On port 443
  TOTP window size:          3
  HOTP window size:          3
  Attempt Skew Adjustment:    No
  Label:                      Unset (using hostname)
  Debug:                      Enabled
  Email OTP enabled:          Yes

Number of configured users:    4
```

Related commands [2fa create user](#)
[2fa delete user](#)
[service 2fa](#)
[show 2fa user](#)

Command changes Version 5.5.2-1.1: command added

show 2fa email-template

Overview Use this command to display the email template used when sending Two-Factor Authentication One-Time-Passwords (2FA email OTP).

Syntax show 2fa email-template

Mode Privileged Exec

Example To display the email template used when sending OTPs, use the command:
awplus# show 2fa email-template

Output The following shows typical output.

Example output from show 2fa email-template

```
Awplus#show 2fa email-template
Subject: %%LABEL%% 2FA Email OTP code

Verification code: %%OTP%%

The verification code will expire in %%EXPIRY_TIME%% minutes.
This is an automated message, please do not reply.
```

Related commands [2fa email-template](#)

Command changes Version 5.5.3-0.1: command added

show 2fa user

Overview Use this command to display information about a Two-Factor Authentication (2FA) user. You can optionally display the user's QR code.

Syntax `show 2fa user <user-name> [qr {ansi|utf8|link}]`

Parameter	Description
<user-name>	The name of the user you want to display.
qr	Display the QR code.
ansi	Display the QR code using ANSI block characters.
utf8	Display the QR code using a UTF-8 mosaic.
link	Display a hyperlink for a QR code generator. Opening the link in a browser will display a QR code. This option passes the string to an online QR code generator (at Google), so it may be a security concern for some installations.

Mode Privileged Exec

Usage notes The QR code displays best in a color mode ANSI or UTF-8 terminal. If your terminal is insufficiently wide, or doesn't have the correct options enabled, you may not get a scannable QR code.

Example1 To display 2FA information including the 2FA mode and the email address for the user name 'otp_user1', use the command:

```
awplus# show 2fa user otp_user1
```

Output 1 **Example output from show 2fa user otp_user1**

```
awplus#show 2fa user otp_user1
Two-Factor Authentication information for user:
Username:      otp_user1
Mode:          Email
Email:         otp_user1@xyz.com
```

Example2 To display 2FA information, and display a hyperlink for a QR code generator, for user name 'test', use the command:

```
awplus# show 2fa user test qr link
```

Output 2 Example output from show 2fa user test qr link

```
awplus#show 2fa user test qr link

Two-Factor Authentication information for user:

Username:      test
Secret:        RXB.....
Mode:          TOTP
OTP URL:       otpauth://totp/test@awplus?secret=RXB.....
Scratch codes:
    70344616
    91312817
    39931705
    89513481
    78647666

The following URL can be used to generate a QR code.
This results in the user key being sent to Google servers.
https://www.google.com/chart?chs=200x200&chld=M|
0&cht=qr&chl=otpauth://totp/test@awplus%3Fsecret
%3DRXBH7KSCH0HWZPG6JFBRR0GPSY
```

Related commands

- 2fa create user email**
- 2fa create user**
- 2fa delete user**
- service 2fa**
- show 2fa**
- show 2fa users**

Command changes Version 5.5.2-1.1: command added

show 2fa users

Overview Use this command to display information about all the users configured with Two-Factor Authentication (2FA) on the device.

Syntax show 2fa users

Mode Privileged Exec

Example To display the information for all configured 2FA users, use the command:
awplus# show 2fa users

Output The following shows typical output.

Example output from show 2fa users

```
awplus#show 2fa users
Two-Factor Authentication users:
Username                               Mode      Last OTP Login
-----
abcd                                   Skip-2FA  -
asasd                                  Skip-2FA  -
clientA1                               TOTP      -
clientA2                               TOTP      -
```

Related commands

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)

Command changes Version 5.5.2-1.1: command added

show debugging 2fa

Overview Use this command to display debugging information for two-factor authentication (2FA).

Syntax show debugging 2fa

Mode Privileged Exec

Example To display debugging information for two-factor authentication, use the command:

```
awplus# show debugging 2fa
```

Output The following shows typical output.

Example output from show 2fa

```
awplus# show debugging 2fa
2FA Debugging Status: on
```

Related commands [debug 2fa](#)
[service 2fa](#)

Command changes Version 5.5.2-1.1: command added

undebug 2fa

Overview Use this command to turn off debug messaging for Two-Factor Authentication (2FA).

Syntax undebug 2fa

Default 2FA debug messaging is off

Mode Privileged Exec

Example To turn off 2FA debug messaging, use the command:
`awplus# undebug 2fa`

Related commands [service 2fa](#)
[show 2fa](#)

Command changes Version 5.5.3-0.1: command added

27 Public Key Infrastructure and Crypto Commands

- Contents**
- **Introduction** on page 1241
 - **crypto key generate rsa** on page 1242
 - **crypto key zeroize** on page 1243
 - **crypto pki authenticate** on page 1244
 - **crypto pki enroll** on page 1245
 - **crypto pki export pem** on page 1246
 - **crypto pki export pkcs12** on page 1247
 - **crypto pki import pem** on page 1249
 - **crypto pki import pkcs12** on page 1251
 - **crypto pki trustpoint** on page 1253
 - **crypto verify** on page 1255
 - **crypto verify bootrom** on page 1257
 - **crypto verify signed** on page 1259
 - **enrollment (ca-trustpoint)** on page 1260
 - **fingerprint (ca-trustpoint)** on page 1262
 - **lifetime** on page 1264
 - **no crypto pki certificate** on page 1265
 - **rsakeypair (ca-trustpoint)** on page 1266
 - **show crypto key mypubkey rsa** on page 1268
 - **show crypto pki certificates** on page 1269
 - **show crypto pki trustpoint** on page 1271
 - **show hash** on page 1273
 - **subject-name (ca-trustpoint)** on page 1274

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](#).

crypto key generate rsa

Overview Use this command to generate a cryptographic public/private key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm.

Syntax `crypto key generate rsa [label <keylabel>] [<1024-16384>]`

Parameter	Description
label	Specify and optional label for the key.
<keylabel>	The name of the key to be created. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. If no label is specified the default value "server-default" is used.
<1024-16384>	The bit length for the key. If no bit length is specified the default of 2048 is used.

Mode Privileged Exec

Usage notes The generated key may be used for multiple server certificates in the system. A key is referenced by its label. A bit length between 1024 and 16384 bits may be specified. Larger bit lengths are more secure, but require more computation time.

The specified key must not already exist.

Example To create a key with the label 'example-server-key' and a bit length of 4096, use the commands:

```
awplus> enable
awplus# crypto key generate rsa label example-server-key 4096
```

Related commands [crypto key zeroize](#)

[rsakeypair \(ca-trustpoint\)](#)

[show crypto key mypubkey rsa](#)

Command changes Version 5.5.2-2.1: Key length increased to 16384

crypto key zeroize

Overview Use this command to delete one or all cryptographic public/private key pairs.

Syntax `crypto key zeroize rsa <keylabel>`
`crypto key zeroize all`

Parameter	Description
<code>rsa</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
<trustpoint>	The name of the trustpoint to be authenticated.

Mode Privileged Exec

Usage notes If the trustpoint's **enrollment** setting is "selfsigned", then this command causes a private key to be generated for the root CA, and a self-signed certificate to be generated based on that key.

If the trustpoint's **enrollment** setting is "terminal", then this command prompts the user to paste a certificate Privacy Enhanced Mail (PEM) file at the CLI terminal. If the certificate is a valid selfsigned CA certificate, then it will be stored as the trustpoint's root CA certificate.

The specified trustpoint must already exist, and its enrollment mode must have been defined.

Example To show the **enrollment** setting of a trustpoint named "example" and then generate a certificate from it, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
awplus(config)# exit
awplus# exit
awplus# crypto pki authenticate example
```

Related commands [crypto pki import pem](#)
[crypto pki trustpoint](#)
[enrollment \(ca-trustpoint\)](#)

crypto pki enroll

Overview Use this command to enroll the local server to the specified trustpoint.
Use the **no** variant of this command to de-enroll the server by removing its certificate

Syntax `crypto pki enroll <trustpoint>`
`no crypto pki enroll <trustpoint>`

Parameter	Description
<code><trustpoint></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 `rsakeypair` parameter for the trustpoint will be included in the server certificate.

If the trustpoint represents a locally self-signed certificate authority, then this command results in the direct generation of the server certificate, signed by the root CA for the trustpoint.

If the trustpoint represents an external certificate authority, then this command results in the generation of a Certificate Signing Request (CSR) file, which is displayed at the terminal in Privacy-Enhanced Mail (PEM) format, suitable for copying and pasting into a file or message. The CSR must be sent to the external CA for processing. When the CA replies with the signed certificate, that certificate should be imported using the `crypto pki import pem` command, to complete the enrollment process.

The specified trustpoint must already exist, and it must already be authenticated.

Example To enroll the local server with the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# crypto pki enroll example
```

Related commands [crypto pki 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
<trustpoint>	The name of the trustpoint for which the certificate and key are to be exported.
ca	If this option is specified, the command exports the root CA certificate and corresponding key.
server	If this option is specified, the command exports the server certificate and corresponding key.
<url>	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 [crypto pki export pem](#)
commands [crypto pki import pkcs12](#)

crypto pki import pem

Overview This command imports a certificate for the given trustpoint from a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred from the specified destination URL, or entered at the terminal.

Syntax `crypto pki import <trustpoint> pem [terminal|<url>]`

Parameter	Description
<trustpoint>	The name of the trustpoint for which the root CA certificate is to be imported.
terminal	Optional parameter, If specified, the command prompts the user to enter (or paste) the PEM file at the terminal. If parameter is specified terminal is assumed by default.
<url>	Optional parameter, If specified, the PEM file is transferred from the specified URL

Default The PEM will be imported from the terminal by default.

Mode Privileged Exec

Usage notes The command is generally used for trustpoints representing external certificate authorities. It accepts root CA certificates, intermediate CA certificates, and server certificates. The system automatically detects the certificate type upon import.

Using this command to import root CA certificates at the terminal is identical to the functionality provided by the `crypto pki authenticate` command, for external certificate authorities. The imported certificate is validated to ensure it is a proper CA certificate.

Intermediate CA certificates are validated to ensure they are proper CA certificates, and that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then intermediate CA certificates may not be imported.

Server certificates are validated to ensure that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then server certificates may not be imported.

The specified trustpoint must already exist. If the imported certificate is self-signed, then no certificates may exist for the trustpoint. Otherwise, the issuer's certificate must already be present for the trustpoint.

Example To import the PEM file for the trustpoint “example” from the terminal, use the following commands:

```
awplus> enable
```

```
awplus# crypto pki import example pem
```

To import the PEM file for the trustpoint “example” from the URL “tftp://server_a/”, use the following commands:

```
awplus> enable
```

```
awplus# crypto pki import example pem tftp://server_a/  
example.pem
```

Related commands

- crypto pki authenticate**
- crypto pki export pem**
- crypto pki trustpoint**

crypto pki import pkcs12

Overview This command imports a certificate and private key for an entity in a trustpoint from a file in PKCS#12 format at the specified URL. The command prompts for a passphrase to decrypt the private key within the file.

Syntax `crypto pki import <trustpoint> pkcs12 {ca|server} <url>`

Parameter	Description
<trustpoint>	The name of the trustpoint for which the certificate and key are to be imported.
ca	If this option is specified, the command imports the root CA certificate and corresponding key.
server	If this option is specified, the command imports the server certificate and corresponding key.
<url>	The source URL for the PKCS#12 file. The format of the 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 [crypto pki export pkcs12](#)
commands [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><trustpoint></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

- [enrollment \(ca-trustpoint\)](#)
- [fingerprint \(ca-trustpoint\)](#)
- [lifetime](#)
- [rsakeypair \(ca-trustpoint\)](#)
- [show crypto pki certificates](#)
- [show crypto pki trustpoint](#)

Command changes Version 5.4.6-1.1: command added to x930 Series
Version 5.4.8-1: command added to x220, XS900MX, x550 Series
Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

crypto verify

Overview Use this command to compare the SHA256 checksum of a file with its correct checksum. This confirms that the file has not been corrupted or interfered with during download. You can verify any kind of file, but you cannot specify a file path, so the file must be stored in the top level of the device's flash memory.



CAUTION: *If a file fails to verify and you believe the file may have been interfered with, we recommend immediately performing a security audit of your network.*

Once the device has verified the file, you can use the **copy running-config startup-config** command to save the file/hash pair in the running configuration. If you do this, the device will verify the file every time it boots up and will take action if the verification fails.

The action taken when verification fails on boot-up depends on the type of file:

- If the boot-up firmware file fails verification, the device will display the following warning message after booting: "% Verification Failed". If this occurs because the saved hash is incorrect, use this command to replace the hash. If this occurs because the firmware file is corrupted or may have been interfered with, ensure that your device is secure, then replace the failed file with a known good file and reboot.
- If you use the **gui** parameter and the GUI fails verification, the device will boot up but the GUI will be disabled (the **service http** command will be disabled).
- If any other file fails verification, the device will display the following warning message after booting: "% Verification Failed"

You can use the **show hash** command to see the current hash of a file.

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

Syntax `crypto verify <filename> <hash-value>`
`crypto verify gui <hash-value>`
`no crypto verify <filename>`

Parameter	Description
<code><filename></code>	The AlliedWare Plus file that you want to verify
<code>gui</code>	Verify the current Device GUI file
<code><hash-value></code>	The known correct checksum of the file. For firmware and GUI files, the correct checksum is listed in the sha256sum file that is available from the Allied Telesis Download Center.

Default	No default
Mode	Global Configuration
Usage notes	All models of a particular series run the same firmware file and therefore have the same checksum for that firmware file. For example, all x930 Series switches have the same checksum. If your network has extremely strict security requirements, such as FIPS compliance, you may need to verify the bootloader on boot-up and use signature verification for the firmware file. To configure these, use the commands crypto verify bootrom and crypto verify signed. These commands make it difficult to upgrade the bootloader or firmware, so only use them if necessary.
Examples	To verify the firmware file for 5.5.3-0.1 on an x930 Series switch, use the commands: <pre>awplus# configure terminal awplus(config)# crypto verify x930-5.5.3-0.1.rel 7f22d8a30c991a4ddc0a2aed47246282b23b4e4a865e07f79795c0959c47de78</pre>
Related commands	crypto verify bootrom crypto verify signed show hash
Command changes	Version 5.5.5-1.1: command available on all AlliedWare Plus devices Version 5.5.3-0.1: gui parameter added; <filename> parameter expanded to cover all file types

crypto verify bootrom

Overview Use this command to compare the SHA256 checksum hash value of a bootloader with its correct checksum. This confirms that the bootloader has not been corrupted or interfered with.

If the verification fails, contact Allied Telesis customer support.

You can use the **write** command to save the hash value to the boot configuration file. The device will verify the checksum every time it boots up and will warn you if it fails the verification.

You can use the **no** variant of this command to remove the bootrom/hash combination from the running configuration.

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

Parameter	Description
<code><hash-value></code>	The known correct checksum of the bootloader. To see the correct hash value, run the command show hash bootrom straight after you first boot the device up, or check the Deployment Guide for the device.

Default No default

Mode Global Configuration

Usage notes Please use this command in accordance with the User Guidance documentation for your required security certification.

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

Examples To verify the bootrom file, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify bootrom
5e80e70b6a2200965abf5f62f72af1bdc1654f3726bdff554afcbd76270c91
```

Note that the hash in this example is an example only; it is not the hash of the device's bootloader.

Related commands [crypto verify](#)
[crypto verify signed](#)
[show hash](#)

Command changes Version 5.5.5-1.1: command available on all AlliedWare Plus devices

crypto verify signed

Overview Use this command to compare the HMAC-SHA checksum hash value of a firmware file with its correct checksum. This confirms that the firmware has not been corrupted or interfered with.

Please use this command in accordance with the User Guidance documentation for your required security certification.

If the verification fails, contact Allied Telesis customer support.

Syntax `crypto verify signed <filename> <hash-value>`

Parameter	Description
<code><filename></code>	The AlliedWare Plus file that you want to verify
<code><hash-value></code>	The known correct checksum of the file. This is a keyed HMAC-SHA hash. This is available in a .sig file, which you can get from your Allied Telesis customer representative.

Default No default

Mode Global Configuration

Usage notes You can use the `write` command to save the hash value to the boot configuration file. The device will verify the checksum every time it boots up and will warn you if it fails the verification.

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

Examples To use signature verification to verify the firmware file for 5.5.3-0.1 on an x930 Series switch, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify signed x930-5.5.3-0.1.rel
3f50420644aebd277dd48b3aee30639801348896fffce231fc5615995ecde5d9
```

Related commands [crypto verify](#)
[crypto verify bootrom](#)
[show hash](#)

Command changes Version 5.5.5-1.1: command available on all AlliedWare Plus devices

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|est|scep}`

Parameter	Description
selfsigned	Sets the enrollment mode for the current trustpoint to selfsigned.
terminal	Sets the enrollment mode for the current trustpoint to terminal.
est	Sets the enrollment mode for the current trustpoint to Secure Transport (EST).
scep	Sets the enrollment mode for the current trustpoint to Simple Certificate Enrollment Protocol (SCEP).

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 enrollment is set to **EST**, the system will contact the EST server specified by **est-url** when the **crypto pki authenticate** command is issued to retrieve the root CA certificate. When the **crypto pki enroll** command is issued, the system will generate a Certificate Signing Request (CSR) for the local server, send it to the EST server for signing, and, if successful, receive the signed server certificate.

If enrollment is set to **SCEP**, the system will contact the SCEP server specified by **scep-url** when the **crypto pki authenticate** command is issued to retrieve the root CA certificate. When the **crypto pki enroll** command is issued, the system will generate a Certificate Signing Request (CSR) for the local server, send it to the SCEP server for signing, and, if successful, receive the signed server certificate.

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**
crypto pki trustpoint
show crypto pki trustpoint

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**
- crypto pki trustpoint**
- show crypto pki trustpoint**

lifetime

Overview Use this command to specify the lifetime of self-signed X.509 certificates as part of configuring the trustpoint. You can specify the certificate lifetime in days (1-3650), months (1-120) or years (1-10).

Use the **no** variant of this command to return to the default lifetime.

Syntax lifetime {days <1-3650>|months <1-120>|years <1-10>}
no lifetime

Parameter	Description
days <1-3650>	Specify the certificate lifetime in days
months <1-120>	Specify the certificate lifetime in months
years <1-10>	Specify the certificate lifetime in years

Default 5 years

Mode Trustpoint Configuration

Example To make the lifetime 10 years for the trustpoint named 'example', use the commands:

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# lifetime years 10
```

Related commands [crypto pki trustpoint](#)
[show crypto pki trustpoint](#)

Command changes Version 5.5.4-0.1: maximum increased to 10 years
Version 5.5.3-2.1: command added with maximum of 5 years

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
<i><trustpoint></i>	The name of the trustpoint.
<i><word></i>	The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings.

Default By default, no fingerprints are pre-accepted for the trustpoint.

Mode Privileged Exec

Usage notes The fingerprint can be found in the output of the **show crypto pki certificates** command. If there are dependent certificates in the trustpoint (i.e., if other certificates were signed by the specified certificate), the command will be rejected.

If the specified certificate is the root CA certificate and the trustpoint represents a locally selfsigned CA, then the corresponding private key is also deleted from the system. Deleting the root CA certificate effectively resets the trustpoint to an unauthenticated state.

Example To delete a certificate with the fingerprint "594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792" from the trustpoint "example", use the following commands:

```
awplus> enable
awplus# no crypto pki certificate example
594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

Related commands no **crypto pki trustpoint**
show crypto pki certificates

rsakeypair (ca-trustpoint)

Overview Use this command to declare which RSA key pair should be used to enroll the local server with the trustpoint. Note that this defines the key pair used with the server certificate, not the key pair used with the root CA certificate.

Use the **no** variant of this command to restore the default value, "server-default".

Syntax `rsakeypair <keylabel> [<1024-4096>]`
`no rsakeypair`

Parameter	Description
<keylabel>	The key to be used with the server certificate for this trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters.
<1024-4096>	The bit length for the key, to be used if the key is implicitly generated during server enrollment.

Default The default value for **keylabel** is "server-default".

The default value for the key bit length is 2048.

Mode Trustpoint Configuration

Usage notes If the label specified does not refer to an existing key created by the **crypto key generate rsa** command, the key will be implicitly generated when the **crypto pki enroll** command is issued to generate the server certificate or the server certificate signing request. The optional numeric parameter defines the bit length for the key, and is only applicable for keys that are implicitly created during enrollment.

This command does not affect server certificates or server certificate signing requests that have already been generated. The trustpoint's server certificate is set to use whatever key pair was specified for the trustpoint at the time the **crypto pki enroll** command is issued.

The default key pair is "server-default". The default bit length is 2048 bits.

Example To configure trustpoint "example" to use the key pair "example-server-key" with a bit length of 2048, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# rsakeypair example-server-key 2048
```

Related commands [crypto key generate rsa](#)
[crypto pki trustpoint](#)
[show crypto pki trustpoint](#)

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 The following shows typical output.

Example output from show crypto key mypubkey rsa

```
awplus#show crypto key mypubkey rsa
-----
RSA Key Pair "example-server-key":
  Key size      : 2048 bits
  Fingerprint   : 1A605D73 C2274CB7 853886B3 1C802FC6 7CDE45FB
  Trustpoints   : example
-----
RSA Key Pair "server-default":
  Key size      : 2048 bits
  Fingerprint   : 34AC4D2D 5249A168 29D426A3 434FFC59 C4A19901
  Trustpoints   : local
```

Related commands [crypto key generate rsa](#)

show crypto pki certificates

Overview Use this command to display information about existing certificates for the specified trustpoint.

Syntax show crypto pki certificates [<trustpoint>]

Parameter	Description
<trustpoint>	The trustpoint for which the certificates are to be shown.

Default By default, the certificates for all trustpoints are shown.

Mode Privileged Exec

Usage notes If no trustpoint is specified, certificates for all trustpoints are shown. The command displays the certificates organized into certificate chains. It starts with the server certificate and then displays its issuer, and continues up the issuer chain until the root CA certificate is reached.

For each certificate, the command displays the certificate type, the subject's distinguished name (the entity identified by the certificate), the issuer's distinguished name (the entity that signed the certificate), the validity dates for the certificate, and the fingerprint of the certificate. The fingerprint is a cryptographic hash of the certificate contents that uniquely identifies the certificate.

The specified trustpoints must already exist.

Example To show the certificates for the trustpoint "example", use the following command:

```
awplus> enable
awplus# show crypto pki certificates example
```

Output The following shows typical output.

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
<i><trustpoint></i>	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 The following shows typical output.

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)
  Lifetime        : 120 months
-----
```

Related **crypto pki trustpoint**
commands **show crypto pki certificates**

show hash

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

Syntax `show hash <filename>`

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

Mode Privileged Exec

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

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

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

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

Output The following shows typical output.

Example output from show hash

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

Command changes Version 5.5.3-0.1: command added

subject-name (ca-trustpoint)

Overview Use this command to specify the distinguished name string that should be used for the subject field in the server certificate, when enrolling the server (generating the server certificate or server certificate signing request).

Syntax subject-name <word>

Parameter	Description
<word>	Specify the subject name as a distinguished name string. Complex strings (e.g., strings containing spaces) should be surrounded with double-quote characters.

Default If no subject name is specified for the trustpoint, then the system automatically builds a name of the form "/O=AlliedWare Plus/CN=xxxx.yyyy.zzz", where "xxxx" is the hostname of the system and "yyy.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 `crypto pki enroll`
commands

28

TACACS+ Commands

- Contents**
- **Introduction** on page 1277
 - **aaa authorization commands** on page 1278
 - **aaa authorization config-commands** on page 1280
 - **authorization commands** on page 1281
 - **ip tacacs source-interface** on page 1283
 - **show tacacs+** on page 1285
 - **tacacs-server host** on page 1287
 - **tacacs-server key** on page 1290
 - **tacacs-server timeout** on page 1292

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACACS+, see the [TACACS+ Feature Overview and Configuration Guide](#).

aaa authorization commands

Overview This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

Syntax `aaa authorization commands <privilege-level> {default|<list-name>} group tacacs+ [none]`
`no aaa authorization commands <privilege-level> {default|<list-name>}`

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: Level = 1: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive Level = 7: All commands that can be accessed by a user with privilege level between 7 and 14 inclusive Level = 15: All commands that can be accessed by a user with privilege level 15
group	Specify the server group where authorization messages are sent. Only the tacacs+ group is available for this command.
tacacs+	Use all TACACS+ servers configured by the tacacs-server host command.
default	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list
none	If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.

Mode Global Configuration

Usage notes TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.
- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

Example To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authorization commands 15 TAC15 group tacacs  
+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authorization commands 7 default group  
tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa authorization commands 15 TAC15
```

Related commands [aaa authorization config-commands](#)
[authorization commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

aaa authorization config-commands

Overview Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

Syntax `aaa authorization config-commands`
`no aaa authorization config-commands`

Default By default, command authorization is disabled on configuration mode commands.

Mode Global Configuration

Usage notes If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

NOTE: *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

Example To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

Related commands [aaa authorization commands](#)
[authorization commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

authorization commands

Overview This command applies a command authorization method list, defined using the **aaa authorization commands** command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

Syntax authorization commands <privilege-level> {default|<list-name>}
no authorization commands <privilege-level>

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: Level = 1: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive Level = 7: All commands that can be accessed by a user with privilege level between 7 and 14 inclusive Level = 15: All commands that can be accessed by a user with privilege level 15
default	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list

Default The **default** method list is applied to each console and VTY line by default.

Mode Line Configuration

Usage notes If the specified method list does not exist users will not be able to execute any commands in the specified method list on the specified VTY lines.

Example To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

Related commands [aaa authorization commands](#)
[aaa authorization config-commands](#)
[tacacs-server host](#)

Command changes Version 5.4.6-2.1: command added

ip tacacs source-interface

Overview This command sets the source interface, or IP address, to use for all TACACS+ packets sent from the device. By default, TACACS+ packets use the source IP address of the egress interface.

Use the **no** variant of this command to remove the source interface configuration and use the source IP address of the egress interface.

Syntax `ip tacacs source-interface {<interface>|<ip-address>}`
`no ip tacacs source-interface`

Parameter	Description
<interface>	Interface name.
<ip-address>	IP address in the dotted decimal format A.B.C.D.

Default The source IP address of outgoing TACACS+ packets default to the IP address of the egress interface.

Mode Global Configuration

Usage notes Setting the source interface ensures that all TACACS+ packets sent from the device will have the same source IP address. Once configured this affects all TACACS+ packets, namely accounting, authentication, and authorization.

If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing TACACS+ packets will default to the IP address of the egress interface.

Example To configure all outgoing TACACS+ packets to use the IP address of the loop-back "lo" interface as the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip tacacs source-interface lo
```

To reset the source interface configuration for all TACACS+ packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip tacacs source-interface
```

Related commands [tacacs-server host](#)
[show tacacs+](#)

Command changes Version 5.4.6-2.1: command added

show tacacs+

Overview This command displays the current TACACS+ server configuration and status.

Syntax show tacacs+

Mode User Exec and Privileged Exec

Example To display the current status of TACACS+ servers, use the command:
awplus# show tacacs+

Output The following shows typical output.

Example output from the show tacacs+ command

TACACS+ Global Configuration	
Source Interface	: not configured
Timeout	: 5 sec
Server Host/ IP Address	Server Status

192.168.1.10	Alive
192.168.1.11	Unknown

Parameters in the output of the show tacacs+ command

Output Parameter	Meaning
Source Interface	IP address of source interface if set with ip tacacs source-interface .
Timeout	A time interval in seconds.
Server Host/IP Address	TACACS+ server hostname or IP address.
Server Status	The status of the authentication port.
	Alive The server is alive.
	Dead The server has timed out.
	Error The server is not responding or there is an error in the key string entered.
	Unknown The server is never used or the status is unknown.
	Unreachable The server is unreachable.
	Unresolved The server name can not be resolved.

Command changes Version 5.4.6-2.1: **Source Interface** parameter added

tacacs-server host

Overview Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

Syntax `tacacs-server host {<host-name>|<ip-address>} [key [8|9] <key-string>]`
`no tacacs-server host {<host-name>|<ip-address>}`

Syntax (VRF-lite) `tacacs-server host {<host-name>|<ip-address>} [vrf <vrf-name>] [key [8|9] <key-string>]`
`no tacacs-server host {<host-name>|<ip-address>} [vrf <vrf-name>]`

Parameter	Description
<i><host-name></i>	Server host name. The DNS name of the TACACS+ server host.
<i><ip-address></i>	The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.
<i>vrf <vrf-name></i>	The name of a VRF instance. Use this to specify the VRF that the TACACS+ server is accessible by. Servers are uniquely identified by their address and VRF, so multiple servers can have the same address or host-name as long as the VRF is different. The default is the global VRF.
key	Set shared secret key with TACACS+ servers.
8	Specifies a string in a DES encrypted format instead of plain text. DES has been deprecated and should not be used. The default encryption format is now AES.
9	Specifies a string in an AES encrypted format instead of plain text. This is the default.
<i><key-string></i>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the tacacs-server key command. If no key value is specified, the global value is used.

Default No TACACS+ server is configured by default.

Mode Global Configuration

Usage A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable
- it cannot communicate with the switch properly due to the switch and the server having different secret keys

Examples To add the server tac1.company.com as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to 'secret' on the TACACS+ server 192.168.1.1, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server tac1.company.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

Examples (VRF-lite) To add the server tac1.company.com as the TACACS+ server host in the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com vrf red
```

To remove the TACACS+ server 192.168.1.1 from the VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host 192.168.1.1 vrf red
```

Related commands

- [aaa accounting commands](#)
- [aaa authentication login](#)
- [tacacs-server key](#)
- [tacacs-server timeout](#)
- [show tacacs+](#)

Command changes

- Version 5.5.4-0.1: DES encrypted format deprecated
- Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

tacacs-server key

Overview This command sets a global secret key for TACACS+ authentication, authorization and accounting. The shared secret text string is used for TACACS+ communications between the switch and all TACACS+ servers.

Note that if no secret key is explicitly specified for a TACACS+ server with the **tacacs-server host** command, this global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to remove the global secret key.

Syntax tacacs-server key [8|9] <key-string>
no tacacs-server key

Parameter	Description
8	Specifies a string in a DES encrypted format instead of plain text. DES has been deprecated and should not be used. The default encryption format is now AES.
9	Specifies a string in an AES encrypted format instead of plain text.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and all TACACS+ servers. This key must match the encryption used on the TACACS+ server.

Default AES encrypted format

Mode Global Configuration

Usage notes Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the **tacacs-server host** command, this global key is used.

Examples To set the global secret key to secret for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

Related commands **tacacs-server host**
show tacacs+

Command changes Version 5.5.4-0.1: DES encrypted format deprecated

tacacs-server timeout

Overview Use this command to specify the TACACS+ global timeout value. The timeout value is how long the device waits for a reply to a TACACS+ request before considering the server to be dead.

Note that this command configures the **timeout** parameter for TACACS+ servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax tacacs-server timeout <seconds>
no tacacs-server timeout

Parameter	Description
<seconds>	TACACS+ server timeout in seconds, in the range 1 to 1000.

Default The default timeout value is 5 seconds.

Mode Global Configuration

Examples To set the timeout value to 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server timeout 3
```

To reset the timeout period for TACACS+ servers to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

Related commands [tacacs-server host](#)
[show tacacs+](#)

Part 5: Network Management

29

AMF and AMF Plus Commands

- Contents**
- **Introduction** on page 1298
 - **application-proxy ip-filter** on page 1299
 - **application-proxy quarantine-vlan** on page 1300
 - **application-proxy redirect-url** on page 1301
 - **application-proxy threat-protection** on page 1302
 - **application-proxy threat-protection send-summary** on page 1304
 - **application-proxy whitelist advertised-address** on page 1305
 - **application-proxy whitelist enable** on page 1306
 - **application-proxy whitelist protection tls** on page 1308
 - **application-proxy whitelist server** on page 1309
 - **application-proxy whitelist trustpoint (deprecated)** on page 1311
 - **area-link** on page 1312
 - **atmf-arealink** on page 1314
 - **atmf-link** on page 1316
 - **atmf amfplus-license-only** on page 1318
 - **atmf area** on page 1320
 - **atmf area password** on page 1322
 - **atmf authorize** on page 1324
 - **atmf authorize provision** on page 1326
 - **atmf backup** on page 1328
 - **atmf backup area-masters delete** on page 1330
 - **atmf backup area-masters enable** on page 1331
 - **atmf backup area-masters now** on page 1332
 - **atmf backup area-masters synchronize** on page 1333
 - **atmf backup bandwidth** on page 1334
 - **atmf backup delete** on page 1335
 - **atmf backup enable** on page 1336
 - **atmf backup guests delete** on page 1337
 - **atmf backup guests enable** on page 1338
 - **atmf backup guests now** on page 1339
 - **atmf backup guests synchronize** on page 1340
 - **atmf backup now** on page 1341
 - **atmf backup redundancy enable** on page 1343
 - **atmf backup server** on page 1344
 - **atmf backup stop** on page 1346
 - **atmf backup synchronize** on page 1347
 - **atmf cleanup** on page 1348

- **atmf container** on page 1349
- **atmf container login** on page 1351
- **atmf controller** on page 1352
- **atmf distribute firmware** on page 1353
- **atmf domain vlan** on page 1355
- **atmf enable** on page 1358
- **atmf group (membership)** on page 1359
- **atmf guest-class** on page 1361
- **atmf log-verbose** on page 1363
- **atmf management subnet** on page 1364
- **atmf management vlan** on page 1367
- **atmf master** on page 1370
- **atmf mtu** on page 1371
- **atmf network-name** on page 1372
- **atmf provision (interface)** on page 1373
- **atmf provision node** on page 1374
- **atmf reboot-rolling** on page 1376
- **atmf recover** on page 1380
- **atmf recover guest** on page 1382
- **atmf recover led-off** on page 1383
- **atmf recover over-eth** on page 1384
- **atmf recovery-server** on page 1385
- **atmf remote-login** on page 1387
- **atmf restricted-login** on page 1389
- **atmf retry guest-link** on page 1391
- **atmf secure-mode** on page 1392
- **atmf secure-mode certificate expire** on page 1394
- **atmf secure-mode certificate expiry** on page 1395
- **atmf secure-mode certificate renew** on page 1396
- **atmf secure-mode enable-all** on page 1397
- **atmf select-area** on page 1399
- **atmf topology-gui enable** on page 1400
- **atmf trustpoint** on page 1402
- **atmf virtual-crosslink** on page 1404
- **atmf virtual-link** on page 1406
- **atmf virtual-link description** on page 1410
- **atmf virtual-link protection** on page 1411
- **atmf working-set** on page 1413
- **bridge-group (amf-container)** on page 1416
- **clear application-proxy threat-protection** on page 1418
- **clear atmf links** on page 1419
- **clear atmf links virtual** on page 1420
- **clear atmf links statistics** on page 1421
- **clear atmf recovery-file** on page 1422
- **clear atmf secure-mode certificates** on page 1423
- **clear atmf secure-mode statistics** on page 1424
- **clone (amf-provision)** on page 1425
- **configure boot config (amf-provision)** on page 1428

- **configure boot system (amf-provision)** on page 1430
- **copy (amf-provision)** on page 1432
- **create (amf-provision)** on page 1434
- **debug atmf** on page 1437
- **debug atmf packet** on page 1439
- **delete (amf-provision)** on page 1442
- **discovery** on page 1444
- **description (amf-container)** on page 1446
- **erase factory-default** on page 1447
- **firmware-url** on page 1448
- **http-enable** on page 1450
- **identity (amf-provision)** on page 1452
- **license-cert (amf-provision)** on page 1455
- **locate (amf-provision)** on page 1457
- **log event-host** on page 1459
- **login-fallback enable** on page 1460
- **modeltype** on page 1461
- **service atmf-application-proxy** on page 1462
- **show application-proxy threat-protection** on page 1463
- **show application-proxy whitelist advertised-address** on page 1465
- **show application-proxy whitelist interface** on page 1466
- **show application-proxy whitelist server** on page 1468
- **show application-proxy whitelist supplicant** on page 1469
- **show atmf** on page 1471
- **show atmf area** on page 1475
- **show atmf area guests** on page 1479
- **show atmf area guests-detail** on page 1481
- **show atmf area nodes** on page 1484
- **show atmf area nodes-detail** on page 1486
- **show atmf area summary** on page 1488
- **show atmf authorization** on page 1489
- **show atmf backup** on page 1492
- **show atmf backup area** on page 1497
- **show atmf backup guest** on page 1499
- **show atmf container** on page 1502
- **show atmf detail** on page 1506
- **show atmf group** on page 1509
- **show atmf group members** on page 1511
- **show atmf guests** on page 1513
- **show atmf guests detail** on page 1515
- **show atmf links** on page 1518
- **show atmf links detail** on page 1520
- **show atmf links guest** on page 1528
- **show atmf links guest detail** on page 1530
- **show atmf links statistics** on page 1534
- **show atmf nodes** on page 1537
- **show atmf provision nodes** on page 1539

- **show atmf recovery-file** on page 1541
- **show atmf secure-mode** on page 1542
- **show atmf secure-mode audit** on page 1545
- **show atmf secure-mode audit link** on page 1546
- **show atmf secure-mode certificates** on page 1547
- **show atmf secure-mode sa** on page 1550
- **show atmf secure-mode statistics** on page 1553
- **show atmf tech** on page 1555
- **show atmf virtual-links** on page 1559
- **show atmf working-set** on page 1561
- **show debugging atmf** on page 1562
- **show debugging atmf packet** on page 1563
- **show running-config atmf** on page 1564
- **state** on page 1565
- **switchport atmf-agentlink** on page 1567
- **switchport atmf-arealink** on page 1569
- **switchport atmf-crosslink** on page 1571
- **switchport atmf-guestlink** on page 1573
- **switchport atmf-link** on page 1575
- **type atmf guest** on page 1576
- **type atmf node** on page 1577
- **undebg atmf** on page 1580
- **username (atmf-guest)** on page 1581

Introduction

Overview This chapter provides an alphabetical reference for AMF and AMF Plus commands. AMF is the Allied Telesis Autonomous Management Framework™, and AMF Plus is an expanded version of AMF. Both AMF and AMF Plus are a suite of features that combine to simplify network management across all supported network equipment from the core to the edge. They also integrate with Vista Manager, our graphical monitoring and management platform.

On the AlliedWare Plus command line, AMF and AMF Plus are identical. The difference between them is in Vista Manager, where AMF Plus includes additional AMF Plus intent-based networking features.

In the rest of this chapter, we use 'AMF' to refer to both AMF and AMF Plus.

AMF master nodes Every AMF network must have at least one master node, which acts as the core of the AMF network. Not all AlliedWare Plus devices are capable of acting as a AMF master. See the [AMF Feature Overview and Configuration Guide](#) for information about master support.

AMF edge AlliedWare Plus CentreCOM® Series switches can only be used as edge switches in an AMF network. The full management power and convenience of AMF is available on these switches, but they can only link to one other AMF node. They cannot form cross-links or virtual links.

AMF naming convention When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command [hostname](#), 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.

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
<i>i</i>	< 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
<i><url></i>	URL to redirect the user to.

Default No URL is configured by default.

Mode Global Configuration

Example To configure a redirect URL, use the command:

```
awplus# application-proxy redirect-url http://my.dom/help.html
```

To remove a redirect URL, use the command:

```
awplus# no application-proxy redirect-url
```

Related commands [application-proxy ip-filter](#)
[application-proxy threat-protection](#)
[clear application-proxy threat-protection](#)
[service atmf-application-proxy](#)
[show application-proxy threat-protection](#)

Command changes Version 5.4.9-0.1: command added

application-proxy threat-protection

Overview Use this command to set the blocking action to take when a threat detected message is received from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable threat protection blocking actions on the port.

Syntax application-proxy threat-protection {drop|link-down|quarantine|log-only}
no application-proxy threat-protection

Parameter	Description
drop	Drop the traffic that generates the threat reports. This is a Layer 2 drop. Note that the device will only drop packets that arrive at the port, not packets sent from the port.
link-down	Take the link down in response to threats, by setting it to error disabled.
quarantine	Move the offending port to a quarantine VLAN.
log-only	Log when a threat is detected.

Default Threat protection is disabled by default.

Mode Interface Configuration

Example To set the threat protection blocking action on port1.0.4 to drop, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy threat-protection drop
```

To disable threat protection blocking actions on port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy threat-protection
```

Related commands **application-proxy quarantine-vlan**
application-proxy threat-protection send-summary
clear application-proxy threat-protection
service atmf-application-proxy
show application-proxy threat-protection

Command changes Version 5.5.2-0.1: added to switch ports on AR series devices
Version 5.4.9-0.1: **log-only** parameter added
Version 5.4.7-2.2: command added

application-proxy threat-protection send-summary

Overview Use this command to send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes. This command can only be performed on an AMF master.

Syntax application-proxy threat-protection send-summary

Mode Privileged Exec

Example To send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes, use the command:

```
awplus# application-proxy threat-protection send-summary
```

Related commands

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [clear application-proxy threat-protection](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)

Command changes Version 5.4.7-2.2: command added

application-proxy whitelist advertised-address

Overview Use this command to register a Layer 3 interface, and the IPv4 address that is attached to this interface, as the advertised application-proxy whitelist address for a device.

Use the **no** variant of this command to stop advertising the Layer 3 interface and its associated IPv4 address.

Syntax application-proxy whitelist advertised-address <interface>
no application-proxy whitelist advertised-address

Parameter	Description
<interface>	Layer 3 interface to configure as the advertised address.

Default No address advertised by default.

Mode Global Configuration

Example To configure the IPv4 address attached to VLAN 1as the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist advertised-address
vlan1
```

To remove the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist advertised-
address
```

Related commands [application-proxy whitelist server](#)
[show application-proxy whitelist advertised-address](#)

Command changes Version 5.4.9-1.1: command added

application-proxy whitelist enable

Overview Use this command to enable application-proxy whitelist based authentication on an interface.

Use the **no** variant of this command to disable the whitelist authentication.

Syntax application-proxy whitelist enable
no application-proxy whitelist enable

Default Application-proxy whitelist is disabled by default.

Mode Interface Configuration

Usage notes When **port-control** is set to **auto**, the 802.1X authentication feature is executed on the interface, but only if the **aaa authentication dot1x** command has been issued.

If you attempt to change the authentication configuration on an interface that has threat protection quarantine configured, you will see the following error message:

```
% portx.x.x: Application Proxy quarantine configuration must be removed before port authentication is changed
```

Before changing the interface's authentication configuration you must either:

- remove the interface's threat protection configuration, or
- shut down the interface.

Example To enable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy whitelist enable
```

To disable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy whitelist enable
```

Related commands **application-proxy whitelist server**
show application-proxy whitelist interface
show application-proxy whitelist server
show application-proxy whitelist supplicant

Command changes Version 5.4.9-0.1: command added

application-proxy whitelist protection tls

Overview Use this command to configure the application-proxy whitelist control channel to use TLS protection. If no trustpoint is specified then TLS will operate without authentication.

Use the **no** variant of this command to stop using TLS.

Syntax application-proxy whitelist protection tls [trustpoint <name>]
no application-proxy whitelist protection tls

Parameter	Description
trustpoint	Specify an optional trustpoint. If no trustpoint is specified then TLS will operate without authentication.
<name>	Name of the trustpoint.

Default TLS is disabled by default.

Mode Global Configuration

Example To configure an AMF application-proxy whitelist to use TLS with the trustpoint 'corpca', use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist protection tls
trustpoint corpca
```

To configure an AMF application-proxy whitelist to stop using TLS, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist protection tls
```

Related commands [application-proxy whitelist enable](#)
[application-proxy whitelist server](#)
[show application-proxy whitelist server](#)

Command changes Version 5.5.0-2.1: command added

application-proxy whitelist server

Overview Use this command to set an AMF master to act as a whitelist authentication proxy between AMF members, acting as Network Access Servers, and an external whitelist RADIUS server.

Use the **no** variant of this command to disable the whitelist proxy functionality.

Syntax application-proxy whitelist server *<ip-address>* key *<key>*
[encrypted] [auth-port *<1-65535>*]
no application-proxy whitelist server

Parameter	Description
<i><ip-address></i>	IPv4 address of the upstream RADIUS server in dotted decimal format A.B.C.D.
key <i><key></i>	Set the shared secret encryption key for communication with the upstream RADIUS server.
encrypted	Means that the password that follows is encoded, not plain text. This parameter is only used in generated configuration files. In configuration files, the device prints encrypted in front of passwords to indicate that it is displaying the encoded password.
auth-port <i><1-65535></i>	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 5.5.3-2.1: **encrypted** parameter added
- Version 5.4.9-0.1: command added

application-proxy whitelist trustpoint (deprecated)

Overview This command has been deprecated. It has been replaced by the **application-proxy whitelist protection tls** command.

This command sets the trustpoint to use when communicating with the external whitelist RADIUS server. This enables RADIUS over TLS (RadSec) protection.

Syntax application-proxy whitelist trustpoint <name>
no application-proxy whitelist trustpoint

Command changes Version 5.4.9-1.1: command added
Version 5.5.0-2.1: command deprecated

area-link

Overview Use this command to create an area-link between a Virtual AMF Appliance (VAA) host controller and an AMF container.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an area-link from a container.

Syntax area-link <area-name>
no area-link

Parameter	Description
<area-name>	AMF area name of the container's area.

Mode AMF Container Configuration

Usage notes The AMF area-link connects the AMF controller on a VAA host to the AMF container. Once a container has been created with the **atmf container** command and an area-link configured with the **area-link** command, it can be enabled using the **state** command.

You can only configure a single area-link on a container. You will see the following message if you try and configure a second one:

% AreaLink already configured for this container

Each container has two virtual interfaces:

- Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, configured using this area-link command.
- Interface eth1, used to connect to the outside world using a bridged L2 network link, configured using the **bridge-group (amf-container)** command.

See the [AMF Feature Overview and Configuration_Guide](#) for more information on these virtual interfaces and links.

Example To create the area-link to “wlg” on container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# area-link wlg
```

To remove an area-link from container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no area-link
```

Related commands [atmf container](#)
[show atmf container](#)

Command changes Version 5.4.7-0.1: command added

atmf-arealink

Overview Use this command to enable an eth interface, on a TQR, ARX or AR-series device, as an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network.

On ARX and AR-Series devices, this command is only available if your network is running in AMF secure mode (see [atmf secure-mode](#) for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF area links that may exist for the selected eth interface.

Syntax atmf-arealink remote-area <area-name> vlan <2-4094>
no atmf-arealink

Parameter	Description
<area-name>	The name of the remote area that the interface is connecting to.
<2-4094>	The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link.

Default No area links are configured

Mode Interface configuration for an eth interface

Usage notes Run this command on the interface at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will synchronize the area information stored on the two nodes.

You can configure multiple area links between two area nodes, but only one area link at any time will be in use. All other area links will block information, to prevent network storms.

NOTE: See the command to configure an AMF area link on an a switch port or link aggregator

Example To configure eth1 as an AMF area link to the 'Auckland' area on VLAN 6, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# atmf-area link remote-area Auckland vlan 6
```

To remove eth1 as an AMF area link, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# no atmf-area link
```

Related commands

- [atmf area](#)
- [atmf area password](#)
- [atmf virtual-link](#)
- [show atmf links](#)

Command changes Version 5.5.0-1.1: command added

atmf-link

Overview Use this command to enable an eth interface on a TQR, ARX or AR-series device as an up/down AMF link.

On ARX and AR-Series devices, this command is only available if your network is running in AMF secure mode (see [atmf secure-mode](#) for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF link that may exist for the selected eth interface.

Syntax atmf-link
no atmf-link

Default No AMF links are configured

Mode Interface configuration for an eth interface

Usage notes Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

On ARX and AR-series devices, if you run the command and AMF secure mode is not enabled, you will see the following error message:

```
Node_1(config)#int eth1
Node_1(config-if)#atmf-link
% Cannot configure eth1 because atmf secure-mode is not enabled.
```

NOTE: See the command to configure an AMF up/down link on an a switch port or link aggregator

Example To configure eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# atmf-link
```

To remove eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# no atmf-link
```


Related commands

- atmf recover over-eth**
- atmf secure-mode**
- show atmf detail**
- show atmf links**
- switchport atmf-link**

Command changes

- Version 5.5.4-0.1: command added on TQ-R series
- Version 5.5.0-1.1: command added

atmf amfplus-license-only

Overview Use this command if you want to use the AMF Plus features in Vista Manager EX, and you have a mixture of AMF and AMF Plus licenses on your master node. This command sets the AMF network to only count **AMF Plus** licensed nodes.

Use the **no** variant of this command to include both AMF and AMF Plus licenses when calculating the number of licensed nodes in an area count.

Syntax atmf amfplus-license-only
no atmf amfplus-license-only

Default The **no** version is the default. That is, consider both AMF and AMF Plus licenses when calculating the number of licensed nodes.

Mode Global Configuration

Usage notes From software version 5.5.2-2.3 onwards, AMF licenses are no longer available to purchase. Instead, AMF Plus licenses become available. Existing AMF licenses remain valid. You only need to change to AMF Plus licenses if you want to manage more nodes, or use the new AMF Plus menu in Vista Manager.



CAUTION: *If the network has more AMF nodes than are licensed with AMF Plus:*

- *AMF Plus will still be enabled in Vista Manager EX (provided there is no AMF license)*
- *any AMF nodes above the license count won't join the AMF network.*

The AMF Plus menu replaces the AOI menu in Vista Manager EX when all the AMF Masters and Controllers have:

- An AMF Plus Controller/Master license on all Masters and Controllers, and
- No AMF Controller/Master licenses applied, or AMF Controller/Master licenses disabled with this command.

Example To set the AMF network to only count AMF Plus licensed nodes, use the commands:

```
awplus#configure terminal
awplus(config)#atmf amfplus-license-only
```

Output The following shows typical output.

Example using atmf amfplus-license-only

```
ATMF Summary Information:
ATMF Status           : Enabled
Network Name          : gtnet
Node Name             : node2
Role                  : Master
Restricted login       : Enabled
Secure Mode           : Disabled
Current ATMF Guests   : 0
Current ATMF Nodes    : 10
Total number of licensed nodes available is 22

node2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
node2(config)#atmf amfplus-license-only
node2(config)#15:41:36 node2 ATMF[1041]: The number of nodes
allowed on this ATMF network is 12

node2(config)#do show atmf
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : gtnet
Node Name             : node2
Role                  : Master
Restricted login       : Enabled
Secure Mode           : Disabled
Current ATMF Guests   : 0
Current ATMF Nodes    : 10
Master is configured to allow only AMFPLUS Licenses
Total number of licensed nodes available is 12
```

Related commands **show atmf**

Command changes Version 5.5.3-0.1: command added

atmf area

Overview This command creates an AMF area and gives it a name and ID number.

Use the **no** variant of this command to remove the AMF area.

This command is only valid on AMF controllers, master nodes and gateway nodes.

Syntax `atmf area <area-name> id <1-4094> [local]`
`no atmf area <area-name>`

Parameter	Description
<code><area-name></code>	The AMF area name. The area name can be up to 15 characters long. Valid characters are: a..zA..Z0..9-_ Names are case sensitive and must be unique within an AMF network. The name cannot be the word "local" or an abbreviation of the word "local" (such as "l", "lo" etc.).
<code><1-4094></code>	An ID number that uniquely identifies this area.
<code>local</code>	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-area link**

Command changes Version 5.5.1-2.1: area **id** maximum increased to 4094

atmf area password

Overview This command sets a password on an AMF area.

Use the **no** variant of this command to remove the password.

This command is only valid on AMF controllers, master nodes and gateway nodes. The area name must have been configured first.

Syntax `atmf area <area-name> password [8] <password>`
`no atmf area <area-name> password`

Parameter	Description
<area-name>	The AMF area name.
8	This parameter is displayed in show running-config output to indicate that it is displaying the password in encrypted form. You should not enter 8 on the CLI yourself.
<password>	The password is between 8 and 32 characters long. It can include spaces.

Mode Global Configuration

Usage notes You must configure a password on each area that an AMF controller communicates with, except for the controller's local area. The areas must already have been created using the **atmf area** command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote AMF area masters

The command **show running-config atmf** will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

Example To give the AMF area named *Auckland* a password of "secure#1" use the following command on the controller:

```
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```
auck-master(config)# atmf area Auckland password secure#1
```

Related **atmf area**
commands **show atmf area**
show atmf area summary
show atmf area nodes
switchport atmf-area link

atmf authorize

Overview On an AMF network, with secure mode enabled, use this command on an AMF master to authorize an AMF node to join the network. AMF nodes waiting to be authorized appear in the pending authorization queue, which can be examined using the [show atmf authorization](#) command with the **pending** parameter.

Use the **no** variant of this command to revoke authorization for an AMF node on an AMF master.

Syntax `atmf authorize {<node-name> [area <area-name>]|all-pending}`
`no atmf authorize <node-name> [area <area-name>]`

Parameter	Description
<node-name>	The name of the node to be authorized or have its authorization revoked.
area	Specify an AMF area.
<area-name>	This is the name of the area the node belongs to.
all-pending	Authorize all nodes in the pending queue.

Mode Privileged Exec

Usage notes On an AMF controller, AMF remote-area masters must be authorized by the controller, and the AMF remote-area masters will also need to authorized access from the AMF controller.

Example To authorize all AMF nodes in the pending authorization queue on an AMF master, use the command:

```
awplus# atmf authorize all-pending
```

To authorize a node called "node2" in remote AMF area "area3", use the command:

```
awplus# atmf authorize node2 area "area3"
```

To authorize a node called "node4" on an AMF master, use the command:

```
awplus# atmf authorize node4
```

To revoke authorization for a node called "node4" on an AMF master, use the command:

```
awplus# no atmf authorize node4
```


Related commands

- atmf secure-mode**
- clear atmf secure-mode certificates**
- show atmf authorization**
- show atmf secure-mode**
- show atmf secure-mode certificates**
- show atmf secure-mode statistics**

Command changes Version 5.4.7-0.3: command added

atmf authorize provision

Overview Use this command from an AMF controller or AMF master to pre-authorize a node on an AMF network running in secure mode. This allows a node to join the AMF network the moment the **atmf secure-mode** command is run on that node.

Use the **no** variant of this command to remove a provisional authorization from an AMF controller or AMF master.

Syntax

```
atmf authorize provision [timeout <minutes>] node <node-name>
interface <interface-name> [area <area-name>]
atmf authorize provision [timeout <minutes>] mac <mac-address>
atmf authorize provision [timeout <minutes>] all
no atmf authorize provision node <node-name> interface
<interface-name> [area <area-name>]
no atmf authorize provision mac <mac-address>
no atmf authorize provision all
```

Parameter	Description
timeout	Timeout for provisional authorization. Authorization for provisioned nodes expires after the timeout period specified.
<minutes>	Timeout in minutes. A value between 1 and 6000 is permissible with the default being 60 minutes.
node	Specify a node to provision by node name.
<node-name>	The name of the node to provisionally authorize.
interface	Specify the interface the node will connect on.
<interface-name>	The name of the interface, this can be a switchport, link aggregator, LACP link, or virtual link.
area	Specify the AMF area.
<area-name>	This is the name of the area the node belongs to.
mac	Specify a node to provision by MAC address.
<mac-address>	Enter a MAC address to provisionally authorize in the format HHHH.HHHH.HHHH.
all	Provision authorization for all secure mode capable nodes.

Default The default timeout is 60 minutes.

Mode Privileged Exec

Example To provisionally authorize all non-secure AMF nodes, use the command:

```
awplus# atmf authorize provision all
```

To authorize a node with a MAC address of 0000.cd28.0880 for 2 hours, use the command:

```
awplus# authorize provision timeout 120 mac 0000.cd28.0880
```

To remove all provisional authorization, on an AMF master, use the command:

```
awplus# no atmf authorize provision all
```

Related commands [show atmf authorization](#)
[show atmf secure-mode](#)

Command changes Version 5.4.7-0.3: command added

atmf backup

Overview This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

Syntax `atmf backup {default|<hh:mm> frequency <1-24>}`

Parameter	Description
default	Restore the default backup schedule.
<hh:mm>	Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock.
backup	Enables AMF backup to external media.
frequency <1-24>	Sets the number of times within a 24 hour period that backups will be taken.

Default Backups run daily at 03:00 AM, by default

Mode Global Configuration

Usage notes Running this command only configures the schedule. To enable the schedule, you should then apply the command **atmf backup enable**.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
```

```
node_1(config)# atmf backup 11:00 frequency 2
```



CAUTION: File names that comprise identical text, but with differing case, such as *Test.txt* and *test.txt*, will not be recognized as being different on FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.

Related commands **atmf backup enable**
atmf backup stop
show atmf backup

atmf backup area-masters delete

Overview Use this command to delete from external media, a backup of a specified node in a specified area.

Note that this command can only be run on an AMF controller.

Syntax `atmf backup area-masters delete area <area-name> node <node-name>`

Parameter	Description
<area-name>	The area that contains the node whose backup will be deleted.
<node-name>	The node whose backup will be deleted.

Mode Privileged Exec

Example To delete the backup of the remote area-master named “well-gate” in the AMF area named Wellington, use the command:

```
controller-1# atmf backup area-masters delete area wellington  
node well-gate
```

Related commands [show atmf backup area](#)

atmf backup area-masters enable

Overview Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

Syntax atmf backup area-masters enable
no atmf backup area-masters enable

Mode Global configuration

Default Remote area backups are disabled by default

Usage notes Use the following commands to configure the remote area-master backups:

- **atmf backup** to configure when the backups begin and how often they run
- **atmf backup server** to configure the backup server.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To enable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

Related commands **atmf backup server**
atmf backup
show atmf backup area

atmf backup area-masters now

Overview Use this command to run an AMF backup of one or more remote area-masters from the AMF controller immediately.

This command is only valid on AMF controllers.

Syntax `atmf backup area-masters now [area <area-name>|area <area-name> node <node-name>]`

Parameter	Description
<area-name>	The area whose area-masters will be backed up.
<node-name>	The node that will be backed up.

Mode Privileged Exec

Example To back up all local master nodes in all areas controlled by controller-1, use the command

```
controller-1# atmf backup area-masters now
```

To back up all local masters in the AMF area named Wellington, use the command

```
controller-1# atmf backup area-masters now area Wellington
```

To back up the local master "well-master" in the Wellington area, use the command

```
controller-1# atmf backup area-masters now area Wellington node well-master
```

Related commands [atmf backup area-masters enable](#)
[atmf backup area-masters synchronize](#)
[show atmf backup area](#)

atmf backup area-masters synchronize

Overview Use this command to synchronize backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

Note that this command is only valid on AMF controllers.

Syntax atmf backup area-masters synchronize

Mode Privileged Exec

Example To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

Related commands [atmf backup area-masters enable](#)
[atmf backup area-masters now](#)
[show atmf backup area](#)

atmf backup bandwidth

Overview This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

NOTE: *This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.*

Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

Syntax atmf backup bandwidth <0-1000>
no atmf backup bandwidth

Parameter	Description
<0-1000>	Sets the bandwidth in kilobytes per second (kBps)

Default The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

Mode Global Configuration

Examples To set an atmf backup bandwidth of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the AMF backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

Related commands [show atmf backup](#)

atmf backup delete

Overview This command removes the backup file from the external media of a specified AMF node.

Note that this command can only be run from an AMF master node.

Syntax `atmf backup delete <node-name>`

Parameter	Description
<code><node-name></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**. 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** 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><node-name></code>	The name of the guest's parent node.
<code><guest-port></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
<i><node-name></i>	The name of the guest's parent node.
<i><guest-port></i>	The port number that connects to the guest node.

Default n/a

Mode Privileged Exec

Example Use the following command to manually trigger the backup of all guests in the AMF network

```
awplus# atmf backup guests now
```

Example To manually trigger the backup of a guest node connected to port 1.0.23 of node1, use the following command:

```
awplus# atmf backup guests now node1 port1.0.23
```

Related commands [show atmf backup guest](#)

atmf backup guests synchronize

Overview This command initiates a manual synchronization of all guest backup file-sets across remote file servers and various redundancy backup media, such as USB storage devices. This facility ensures that each device contains the same backup image files. Note that this backup synchronization process will occur as part of the regular backups scheduled by the **atmf backup** command.

Syntax atmf backup guests synchronize

Default n/a

Mode User Exec/Privileged Exec

Example To synchronize backups across remote file servers and storage devices, use the command:

```
Node1#atmf backup guests synchronize
```

Related commands **atmf backup redundancy enable**

show atmf guests

atmf backup guests enable

atmf backup now

Overview This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

Note that this command can only be run on an AMF master node.

Syntax atmf backup now [<nodename>]

Parameter	Description
<nodename> or <hostname>	The name of the AMF member to be backed up, as set by the command hostname . Where no name has been assigned to this device, then you must use the default name, which is the word "host", then an underscore, then (without a space) the MAC address of the device to be backed up. For example host_0016_76b1_7a5e. Note that the node-name appears as the command Prompt when in Privileged Exec mode.

Default A backup is initiated for all nodes on the AMF (but stored on the master nodes).

Mode Privileged Exec

Usage notes Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

NOTE: The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in Example 4 below.

Example 1 In this example, an AMF member has not been assigned a host name. The following command is run on the AMF_Master_2 node to immediately backup the device that is identified by its MAC address of 0016.76b1.7a5e:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

NOTE: When a host name is derived from its MAC address, the syntax format entered changes from XXXX.XXXX.XXXX to XXXX_XXXX_XXXX.

Example 2 In this example, an AMF member has the host name, **office_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device's master node named **AMF_Master_2** and initiates an immediate backup on the device named **office_annex**.

Example 3 To initiate from AMF_master_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

Example 4 To initiate an immediate backup of the node with the host-name "office_annex" and store the configuration on both masters, use the following process:

From the AMF_master_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
=====
AMF_Master_1, AMF_Master_2
=====

Working set join
```

Backup the AMF member with the host name, **office_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

Related commands

- atmf backup**
- atmf backup stop**
- hostname**
- show atmf backup**

atmf backup redundancy enable

Overview This command is used to enable or disable AMF backup redundancy.

Syntax atmf backup redundancy enable
no atmf backup redundancy enable

Default Disabled

Mode Global Configuration

Usage notes If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To enable AMF backup redundancy, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no atmf backup redundancy enable
```

Related commands [atmf backup synchronize](#)
[show atmf backup](#)
[show atmf backup area](#)

atmf backup server

Overview This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

Syntax `atmf backup server id {1|2} <hostlocation> username <username> [path <path>|port <1-65535>]`
`no atmf backup server id {1|2}`

Parameter	Description
id	Remote server backup server identifier.
{1 2}	The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server.
<hostlocation>	Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).
username	Configure the username to log in with on the selected remote file server.
<username>	The selected remote file server's username.
path	The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.
<path>	The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.
port	The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.
<1-65535>	A TCP port within the specified range.

Defaults Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

Mode Global Exec

Usage notes The hostname and username parameters must both be configured.

Examples To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username
backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

Related commands [show atmf backup](#)

atmf backup stop

Overview Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

Syntax `atmf backup stop`

Mode Privileged Exec

Usage notes This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

Related commands

- [atmf backup](#)
- [atmf backup enable](#)
- [atmf backup now](#)
- [show atmf backup](#)

atmf backup synchronize

Overview For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

Syntax atmf backup synchronize

Mode Privileged Exec

Example When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

Related commands

- atmf backup enable**
- atmf backup redundancy enable**
- show atmf**
- show atmf backup**

atmf cleanup

Overview This command is an alias to the **erase factory-default** command.

atmf container

Overview Use this command to create or update an AMF container on a Virtual AMF Appliance (VAA) virtual machine.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an AMF container.

Syntax `atmf container <container-name>`
`no atmf container <container-name>`

Parameter	Description
<code><container-name></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 \(amf-container\)](#)
[description \(amf-container\)](#)
[show atmf container](#)
[state](#)

Command changes Version 5.4.7-0.1: command added

atmf container login

Overview Use this command to login to an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Syntax atmf container login <container-name>

Parameter	Description
<container-name>	The name of the AMF container you wish to login into.

Mode Privileged Exec

Usage notes If you try to login to a AMF container that has not been created, or is not running, you will see the following message:

% Container does not exist or is not running.

To exit from a container and return to the host VAA press <Ctrl+a q>.

Example To login to container "vac-wlg-1", use the command:

```
awplus# atmf container login vac-wlg-1
```

You will then be presented with a login screen for that container:

```
Connected to tty 1
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

vac-wlg-1 login: manager
Password: friend

AlliedWare Plus (TM) 5.4.7 02/03/17 08:46:12

vac-wlg-1>
```

Related commands [atmf container](#)
[show atmf container](#)

Command changes Version 5.4.7-0.1: command added

atmf controller

Overview Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

AMF controller is a licensed feature. The number of areas supported on a controller depends on the license installed on that controller.

Use the **no** variant of this command to remove the AMF controller functionality.

Syntax atmf controller
no atmf controller

Mode Global configuration

Usage notes If a valid AMF controller license is not available on the device, the device will accept this command but will not act as a controller until you install a valid license. The following message will warn you of this:

"An AMF Controller license must be installed before this feature will become active"

NOTE: *If the AMF controller functionality is removed from a device using the command then the device must be rebooted if it is to function properly as an AMF master.*

Example To configure the node named *controller-1* as an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named *controller-1* from being an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

Related commands [atmf area](#)
[show atmf](#)

atmf distribute firmware

Overview This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash on the new location.

The new release name is updated using the **boot system** command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the command should be used on the working-set.

Syntax atmf distribute firmware <filename>

Parameter	Description
<filename>	The filename and path of the file. See the File Management Feature Overview and Configuration Guide for valid syntax.

Mode Privileged Exec

Examples To upgrade nodes in a AMF network with a predefined AMF group called 'teams', use the following command:

Team1# atmf working-set group teams

```
=====
Team1, Team2, Team3:
=====
Working set join
```

ATMF_NETWORK[3]# atmf distribute firmware card:*.rel

```
Retrieving data from Team1
Retrieving data from Team2
Retrieving data from Team3

ATMF Firmware Upgrade:

Node Name          New Release File          Status
-----
Team1              x510-5.4.7-1.1.rel        Release ready
Team2              x930-5.4.7-1.1.rel        Release ready
Team3              x930-5.4.7-1.1.rel        Release ready
Continue the rolling reboot ? (y/n):y
=====
Copying Release    : x510-5.4.7-1.1.rel to Team1
Updating Release   : x510-5.4.7-1.1.rel information on Team1
=====
Copying Release    : x930-5.4.7-1.1.rel to Team2
Updating Release   : x930-5.4.7-1.1.rel information on Team2
=====
Copying Release    : x930-5.4.7-1.1.rel to Team3
Updating Release   : x930-5.4.7-1.1.rel information on Team3
=====
New firmware will not take effect until nodes are rebooted.
=====

ATMF_NETWORK[3]#
```

Related [atmf working-set commands](#)

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 .*

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
<i><group-list></i>	A list of group names. These should be entered as a comma delimited list without spaces. Names can contain alphanumeric characters, hyphens and underscores.

Mode Global Configuration

Usage notes You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the **atmf group (membership)** command to all members of the working set.

Example 1 To specify the device to become a member of AMF groups named *marketing*, *sales*, and *building_2*, use the following commands:

```
node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2
```

Example 2 To add the nodes *member_node_1* and *member_node_2* to groups *building1* and *sales*, first add the nodes to the working-set:

```
master_node# atmf working-set member_node_1,member_node_2
```

This command returns the following output confirming that the nodes *member_node_1* and *member_node_2* are now part of the working-set:

```
=====
member_node_1, member_node_2
=====

Working set join
```

Then add the members of the working set to the groups:

```
atmf-net[2]# configure terminal
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
=====
member_node_1
=====

AMF group information
building1, sales
```

Related commands [show atmf group](#)
[show atmf group members](#)

atmf guest-class

Overview This modal command creates a guest-class. Guest-classes are modal templates that can be applied to selected guest types. Once you have created a guest-class, you can select it by entering its mode. From here, you can then configure a further set of operational settings specifically for the new guest-class.

These settings can then all be applied to a guest link by running the **switchport atmf-guestlink** command. The following settings can be configured from each guest class mode:

- discovery method
- model type
- http-enable setting
- guest port, user name, and password

The **no** variant of this command removes the guest-class. Note that you cannot remove a guest-class that is assigned to a port.

Syntax atmf guest-class *<guest-class-name>*
no atmf guest-class *<guest-class-name>*

Parameter	Description
<i><guest-class-name></i>	The name assigned to the guest-class type. This can be chosen from an arbitrary string of up to 15 characters.

Mode Global Configuration

Example To create a guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class camera
node1(config-atmf-guest)#
```

To remove the guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# no atmf guest-class camera
```

Related commands [show atmf area guests](#)
[discovery](#)
[firmware-url](#)
[http-enable](#)

username (atmf-guest)

modeltype

switchport atmf-guestlink

show atmf links guest

show atmf guests

login-fallback enable

atmf log-verbose

Overview 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 .*

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><name></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><nodename></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, dynamic channel group or an Eth port on an AR-Series device.

Usage notes The port should be configured as an AMF link or cross link and should be 'down' to add or remove a provisioned node.

Example To provision an AMF node named node1 for port1.0.1, use the commands:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

Related commands

- `atmf provision node`
- `clone (amf-provision)`
- `configure boot config (amf-provision)`
- `configure boot system (amf-provision)`
- `copy (amf-provision)`
- `create (amf-provision)`
- `delete (amf-provision)`
- `identity (amf-provision)`
- `license-cert (amf-provision)`
- `locate (amf-provision)`
- `show atmf provision nodes`
- `show atmf links`
- `switchport atmf-link`
- `switchport atmf-crosslink`

atmf provision node

Overview Use this command to provision a replacement node for a specified interface. Node provisioning is effectively the process of creating a backup file-set on a master node that can be loaded onto a provisioned node some time in the future. This file-set is created just as if the provisioned node really existed and was connected to the network. Typically these comprise configuration, operating system, and license files etc.

You can optionally provision a node with multiple device-type backups. When a device is then attached to the network, AMF uses its device-type to find the correct configuration to use. For example you can create an x510 and an x530 provisioning configuration for a node called 'node1' and if either an x510 or an x530 is attached to that node the appropriate configuration will be used.

Use the **no** variant of this command to remove a provisioned node.

Syntax `atmf provision node <nodename> [device <device-type>]`
`no atmf provision node <nodename> [device <device-type>]`

Parameter	Description
<nodename>	The name of the provisioned node that will appear on the AMF network.
device	Optionally specify a device type.
<device-type>	Any valid device type e.g. AR3050s, ie200, x950. For a full list of valid device types use the command atmf provision node <nodename> device ? .

Mode Privileged Exec

Usage notes This command creates the directory structure for the provisioned node's file-set. It also switches to the AMF provision node prompt so that the nodes backup file-set can be created or updated. This is typically done with the **create (amf-provision)** or **clone (amf-provision)** commands.

For more information on AMF provisioning, see the [AMF Feature Overview and Configuration Guide](#)..

Example To configure node named 'node1', use the command:

```
awplus# atmf provision node node1  
awplus(atmf-provision)#
```

To configure a node named 'node1' for device type 'x530', use the command:

```
awplus# atmf provision node node1 device x530  
awplus(atmf-provision)#
```

Related commands

- atmf provision (interface)**
- clone (amf-provision)**
- configure boot config (amf-provision)**
- configure boot system (amf-provision)**
- copy (amf-provision)**
- create (amf-provision)**
- delete (amf-provision)**
- identity (amf-provision)**
- license-cert (amf-provision)**
- locate (amf-provision)**
- show atmf provision nodes**

Command changes Version 5.4.9-0.1: command added

atmf reboot-rolling

Overview This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the `url` parameter, you can also upgrade your devices' software one AMF node at a time.

The **force** parameter forces the rolling reboot to continue even if a previous node does not rejoin the AMF network. Without the **force** parameter, the unsuitable node will time-out and the rolling reboot process will stop. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

Syntax `atmf reboot-rolling [force] [<url>]`

Parameter	Description
<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><url></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 `usb:/5.5.2-2/x*-5.5.2-2-*.rel` will select from the folder `usb:/5.5.2-2` the latest file that matches the selection `x(wildcard)-5.5.2-2-(wildcard).rel`. Because `x*` is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

Entry	Used when loading software
<code>card:*.rel:</code>	from an SD card
<code>tftp:<ip-address>:</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 x530 nodes in an AMF network, use the commands:

```
Bld2_Floor_1# atmf working-set group x530
```

This command returns the following type of screen output:

```
=====
node1, node2, node3:
=====

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x530

=====
SW_Team1, SW_Team2, SW_Team3:
=====

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

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 on all relevant devices in the network, when the new files are for 5.5.2-2.1 and are stored in a directory on a USB stick, use the commands:

```
Node_1# atmf working-set group all
ATMF_NETWORK[9]# atmf reboot-rolling usb:/5.5.2-2/
x*-5.5.2-2*.rel
```

ATMF Rolling Reboot Nodes:			
Node Name	Timeout (Minutes)	New Release File	Status

SW_Team1	8	x530-5.5.2-2.1.rel	Release Ready
SW_Team2	10	x530-5.5.2-2.1.rel	Release Ready
SW_Team3	8	---	Not Supported
HW_Team1	6	---	Incompatible
Bld1_Floor_2	2	x930-5.5.2-2.1.rel	Release Ready
Bld1_Floor_1	4	---	Incompatible
Building_1	2	---	Incompatible
Building_2	2	x950-5.5.2-2.1.rel	Release Ready
Continue upgrading releases ? (y/n):			

atmf recover

Overview This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced.

Syntax `atmf recover [<node-name> master <node-name>]`
`atmf recover [<node-name> controller <node-name>]`

Parameter	Description
<code><node-name></code>	The name of the device whose configuration is to be recovered or replicated.
<code>master <node-name></code>	The name of the master device that holds the required configuration information. Note that although you can omit both the node name and the master name; you cannot specify a master name unless you also specify the node name.
<code>controller <node-name></code>	The name of the controller that holds the required configuration information. Note that although you can omit both the node name and the controller name; you cannot specify a controller name unless you also specify the node name.

Mode Privileged Exec

Usage notes The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the *<node-name>* parameter, and you can specify the name of the master node or controller holding the configuration file.

If the *<node-name>* parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.

Example To recover the AMF node named Node_10 from the AMF master node named Master_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

Related commands [atmf backup stop](#)
[show atmf backup](#)
[show atmf](#)

atmf recover guest

Overview Use this command to initiate a guest node recovery or replacement by reloading its backup file-set that is located within the AMF backup system. Note that this command must be run on the edge node device that connects to the guest node.

Syntax atmf recover guest [*<guest-port>*]

Parameter	Description
<i><guest-port></i>	The port number that connects to the guest node.

Mode User Exec/Privileged Exec

Example To recover a guest on node1 port1.0.1, use the following command
`node1# atmf recover guest port1.0.1`

Related commands [show atmf backup guest](#)

atmf recover led-off

Overview This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the [AMF Feature Overview and Configuration Guide](#).

Syntax atmf recover led-off

Default Normal operational mode

Mode Privileged Exec

Example To revert the LEDs on Node1 from recovery mode display to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

Related commands [atmf recover](#)

atmf recover over-eth

Overview Use this command to enable AMF recovery over an AR-series device's Eth port. This setting persists even after restoring a device to a 'clean' state with the **erase factory-default** or **atmf cleanup** command.

Use the **no** variant of this command to disable AMF recover over an Eth port.

Syntax atmf recover over-eth
no atmf recover over-eth

Default Eth ports cannot be used for recovery.

Mode Privileged Exec

Usage notes AMF links over Eth ports are only available if your network is running in AMF secure mode (see **atmf secure-mode** for more information on AMF secure mode).

Example To enable AMF recovery over an Eth port, use the command:

```
awplus# atmf recover over-eth
```

To disable AMF recovery over an Eth port, use the commands:

```
awplus# no atmf recover over-eth
```

Related commands **atmf-link**
atmf recover
atmf secure-mode
erase factory-default
show atmf detail

Command changes Version 5.5.0-1.1: command added

atmf recovery-server

Overview Use this command on an AMF master to process recovery requests from isolated AMF nodes. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This option allows these nodes, which have no AMF neighbors, to be identified for recovery or provisioning purposes. They are identified using an identity token which is stored on the AMF master.

Use the **no** variant of this command to disable processing of recovery requests from isolated AMF nodes.

Syntax atmf recovery-server
no atmf recovery-server

Default Recovery-server is disabled by default.

Mode Global Configuration

Usage notes Once **recovery-server** is enabled on an AMF network, the next time an isolated node is backed up its identity token will be stored in the AMF master's database. Should the device fail it can then be replaced and auto-recovery will occur as long as:

- the AMF master is accessible to the isolated node, and
- either, a DHCP server is configured to send the Uniform Resource Identifier (URI) of the AMF master to the recovering node, or
- a DNS server is configured to resolve the default recovery URI (<https://amfrecovery.alliedtelesis.com>) to the IP address of the AMF master.

Provisioning of isolated nodes is achieved by creating an identity token for the new node using the **identity (amf-provision)** command.

See the **AMF Feature Overview and Configuration Guide** for information on preparing your network for recovering or provisioning isolated nodes.

Example To enable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# atmf recovery-server
```

To disable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf recovery-server
```

- Related commands

atmf backup

atmf cleanup

identity (amf-provision)

atmf virtual-link
- Command changes

Version 5.4.7-2.1: command added

atmf remote-login

Overview Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

Syntax `atmf remote-login [user <name>] <nodename>`

Parameter	Description
<name>	The name of a user on the remote node.
<nodename>	The name of the remote AMF node you are connecting to.

Mode Privileged Exec (This command will only run at privilege level 15)

Usage notes You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (e.g. device reboot) you will be returned to the originating node.

You can create additional user accounts on nodes. AMF's goal is to provide a uniform management plane across the whole network, so we recommend you use the same user accounts on all the nodes in the network.

In reality, though, it is not essential to have the same accounts on all the nodes. Users can remote login from one node to a second node even if they are logged into the first node with a user account that does not exist on the second node (provided that **atmf restricted-login** is disabled and the user account on the first node has privilege level 15).

Moreover, it is possible to use a RADIUS or TACACS+ server to manage user authentication, so users can log into AMF nodes using user accounts that are present on the RADIUS or TACACS+ server, and not present in the local user databases of the AMF nodes.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

If you disconnect from the VTY session without first exiting from the AMF remote session, the device will keep the AMF remote session open until the **exec-timeout** time expires (10 minutes by default). If the exec-timeout time is set to infinity (**exec-timeout 0 0**), then the device is unable to ever close the remote session. To avoid this, we recommend you use the **exit** command to close AMF remote sessions, instead of closing the associated VTY sessions. We also recommend you avoid setting the exec-timeout to infinity.

Example To remotely login from node Node10 to Node20, use the following command:

```
Node10# atmf remote-login node20
```

```
Node20>
```

To close the session on Node20 and return to Node10's command line, use the following command:

```
Node20# exit
```

```
Node10#
```

In this example, user User1 is a valid user of node5. They can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user User1 node3
```

```
node3> enable
```

Related commands [atmf restricted-login](#)

Command changes Version 5.4.6-2.1: changes to AMF user account requirements

atmf restricted-login

Overview By default, users who are logged into any node on an AMF network are able to manage any other node by using either working-sets or an AMF remote login. If the access provided by this feature is too wide, or contravenes network security restrictions, it can be limited by running this command, which changes the access so that:

- users who are logged into non-master nodes cannot execute any commands that involve working-sets, and
- from non-master nodes, users can use remote-login, but only to login to a user account that is valid on the remote device (via a statically configured account or RADIUS/TACACS+). Users are also required to enter the password for that user account.

Once entered on any AMF master node, this command will propagate across the network.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

Syntax atmf restricted-login
no atmf restricted-login

Mode Privileged Exec

Default Master nodes operate with **atmf restricted-login** disabled.
Member nodes operate with **atmf restricted-login** enabled.

NOTE: *The default conditions of this command vary from those applied by its “no” variant. This is because the restricted-login action is only applied by nodes, and in the absence of a master node, the default is to apply the restricted action to all nodes with AMF configured.*

Usage notes In the presence of a **master** node, its default of **atmf restricted-login disabled** will propagate to all its member nodes. Similarly, any change in this command’s status that is made on a master node, will also propagate to all its member nodes

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Restricted-login must be enabled on AMF areas with more than 120 nodes.

Example To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

Related commands [atmf remote-login](#)
[show atmf](#)

Command changes Version 5.4.6-2.1: changes to AMF user account requirements

atmf retry guest-link

Overview Use this command to retry an AMF guest-link by restarting AMF guest discovery on a port if it is currently in the failed state.

If no port is specified then all configured AMF guest-link ports that are in the failed state are retried.

If a port is specified then that port will only be retried if it is both:

- configured as an AMF guest-link, and
- it is currently in the failed state.

Syntax `atmf retry guest-link [<interface>]`

Parameter	Description
<code><interface></code>	Name of the interface the guest-link you want to retry is configured on.

Mode Privileged Exec

Example To retry all configured AMF guest-link currently in a failed state, use the command:

```
awplus# atmf retry guest-link
```

To retry an AMF guest-link configured on port1.0.2 currently in a failed state, use the command:

```
awplus# atmf retry guest-link port1.0.2
```

Related commands [show atmf links guest](#)
[switchport atmf-guestlink](#)

atmf secure-mode

Overview Use this command to enable AMF secure mode on an AMF node. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before 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 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><node-name></code>	Name of the AMF node you want to expire the certificate for.
<code>area</code>	Specify an AMF area.
<code><area-name></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
<days>	Length of time, in days, that an AMF secure mode certificate remains valid. A value between 1 and 365.
infinite	The authorization certificate does not expire, in other words AMF nodes stay authorized indefinitely.

Default The default expiry time is 180 days.

Mode Global Configuration

Example To set AMF secure mode certificate expiry to 7 days, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf secure-mode certificate expiry 7
```

To set AMF secure mode certificates to never expire, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf secure-mode certificate expiry infinite
```

To reset the certificate expiry to 180 days, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no atmf secure-mode certificate expiry
```

Related commands [atmf secure-mode](#)
[show atmf secure-mode](#)
[show atmf secure-mode certificates](#)

Command changes Version 5.4.7-0.3: command added

atmf secure-mode certificate renew

Overview Use this command to force all local certificates to expire and be renewed on an AMF secure mode network.

Secure mode certificates renew automatically but this command could be used to renew a certificate in a situation where the automatic renewal may happen while the device is not attached to the AMF network.

Syntax atmf secure-mode certificate renew

Mode Privileged Exec

Example To renew a local certificate on a AMF member or AMF master, use the command:

```
awplus# atmf secure-mode certificate renew
```

Related commands [show atmf secure-mode certificates](#)
[show atmf secure-mode statistics](#)

Command changes Version 5.4.7-0.3: command added

atmf secure-mode enable-all

Overview Use this command to enable AMF secure mode on an entire network. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before an AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once this command is run on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

This command can only be run on an AMF master.

Use the **no** variant of this command to disable AMF secure mode on an entire network.

Syntax atmf secure-mode enable-all
no atmf secure-mode enable-all

Default Secure mode is disabled by default.

Mode Privileged Exec

Usage notes When an AMF network is running in AMF secure mode the **atmf restricted-login** feature is automatically enabled. This restricts the **atmf working-set** command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Running **atmf secure-mode enable-all**:

- Groups all AMF members in a working set.
- Executes **clear atmf secure-mode certificates** on the working set of members, which removes existing secure mode certificates from all the nodes.
- Groups all the AMF masters in a working set.
- Executes **atmf authorize provision all** on the working set of masters, so all masters provision all nodes.
- Groups all AMF nodes in a working set.
- Runs a script which executes **atmf secure-mode** and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

Running **no atmf secure-mode enable-all**:

- Groups all AMF nodes in a working set.
- Runs a script which executes **no atmf secure-mode** and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

NOTE: Enabling or disabling secure mode on the network saves the running-config on every device.

Example To enable AMF secure mode on the entire network, use the command:

```
awplus# atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
Total number of nodes 21
21 nodes support secure-mode

Enable secure-mode across the AMF network ? (y/n): y
```

To disable AMF secure mode on the entire network, use the command:

```
awplus# no atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
% Warning: All security certificates will be deleted.
Disable secure-mode across the AMF network ? (y/n): y
```

Related commands **show atmf**

Command changes Version 5.4.7-0.3: command added

atmf select-area

Overview Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The **no** variant of this command disconnects you from the remote area-master.

Syntax `atmf select-area {<area-name>|local}`
`no atmf select-area`

Parameter	Description
<code><area-name></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
```

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

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

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

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

Related **atmf enable**
commands **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><trustpoint-name></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.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a virtual crosslink.

Syntax `atmf virtual-crosslink id <local-id> ip <local-ip> remote-id <remote-id> remote-ip <remote-ip>`
`atmf virtual-crosslink id <local-id> ip <local-ip> remote-id <remote-id> remote-host <domainname>`
`no atmf virtual-crosslink id <local-id>`

Parameter	Description
<code>id <local-id></code>	ID of the local tunnel port, a value between 1 and 4094.
<code>ip <local-ip></code>	IPv4 address of the local tunnel port in a.b.c.d format.
<code>remote-id <remote-id></code>	ID of the remote tunnel port, a value between 1 and 4094.
<code>remote-ip <remote-ip></code>	IPv4 address of the remote tunnel port in a.b.c.d format.
<code>remote-host <domainname></code>	The domain name of the remote node.

Default No AMF virtual crosslinks are created by default.

Mode Global Configuration

Usage notes This command allows a virtual tunnel to be created between two remote sites over a Layer 3 link. The tunnel encapsulates AMF packets and allows them to be sent transparently across a Wide Area Network (WAN) such as the Internet.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID, and a remote IP address or domain name. Each side of the tunnel must be configured with the same, but mirrored parameters.

NOTE: *Virtual crosslinks are not supported on AMF container masters, therefore if multiple tenants on a single VAA host are configured for secure mode, only a single AMF master is supported per area.*

Example To setup a virtual link from a local site, 'siteA', to a remote site, 'siteB', (assuming there is already IP connectivity between the sites), run the following commands at the local site:

```
siteA# configure terminal
siteA(config)# atmf virtual-crosslink id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1
```

At the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# atmf virtual-crosslink id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1
```

To remove this virtual crosslink, run the following commands on the local site:

```
siteA# configure terminal
siteA(config)# no atmf virtual-crosslink id 5
```

On the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# no atmf virtual-crosslink id 10
```

Related commands [atmf virtual-crosslink](#)
[show atmf links](#)
[switchport atmf-crosslink](#)

Command changes Version 5.5.2-0.1: **remote-host** parameter added
Version 5.4.7-0.3: command added

atmf virtual-link

Overview This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove the specified virtual link.

Syntax

```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>  
remote-ip <a.b.c.d> [remote-area <area-name>]  
atmf virtual-link id <1-4094> interface <interface-name> remote-  
id <1-4094> remote-ip <a.b.c.d> [remote-area <area-name>]  
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>  
remote-host <domainname> [remote-area <area-name>]  
atmf virtual-link id <1-4094> interface <interface-name> remote-  
id <1-4094> remote-host <domainname> [remote-area <area-name>]  
no atmf virtual-link id <1-4094>
```

Parameter	Description
id <1-4094>	ID of the local tunnel point, in the range 1 to 4094.
ip <a.b.c.d>	Specify the local IP address of the local interface for the virtual-link (alternatively you can specify the interface's name, see below).
interface <interface-name>	Specify the local interface name for the virtual-link. This allows you to use a dynamic, rather than a static, local IP address.
remote-id <1-4094>	The ID of the (same) tunnel that will be applied by the remote node. Note that this must match the local-id that is defined on the remote node. This means that (for the same tunnel) the local and remote tunnel IDs are reversed on the local and remote nodes.
remote-ip <a.b.c.d>	The IP address of the remote node.
remote-host <domainname>	The domain name of the remote node.
remote-area <area-name>	The name of the remote area connected to this virtual-link.

Mode Global Configuration

Usage notes The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address or domain name. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.

If an interface acquires its IP address dynamically then the local side of the tunnel can be specified by using the interface's name instead of using its IP address. When using a dynamic local address the remote address of the other side of the virtual-link must be configured with either:

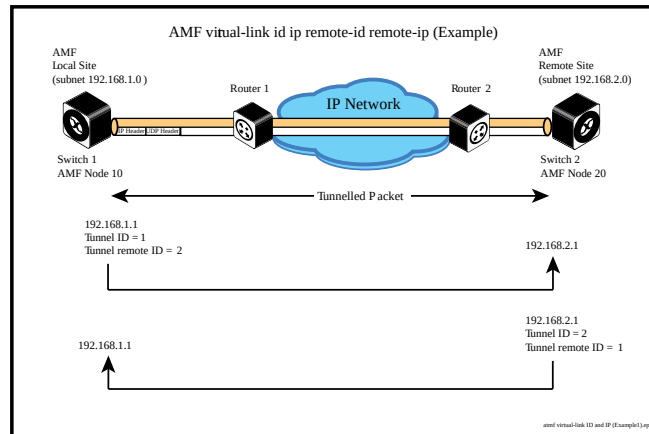
- the IP address of the NAT device the dynamically configured interface is behind, or
- 0.0.0.0, if the virtual-link is configured as a secure virtual-link.

For instructions on how to configure dynamic IP addresses on virtual-links, see the [AMF Feature Overview and Configuration Guide](#).

The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

NOTE: *AMF cannot achieve zero touch replacement of the remote device that terminates the tunnel connection, because you must pre-configure the local IP address and tunnel ID on that remote device.*

Example 1 Use the following commands to create the tunnel shown in the figure below.



AMF virtual link example

```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1 remote-id 2 remote-ip 192.168.2.1
Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1 remote-id 1 remote-ip 192.168.1.1
```

Example 2 To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
```

```
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1 remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
```

```
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1 remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

Before you can apply the above **atmf virtual-link** command, you must configure the area names *SiteB-AREA* and *SiteA-AREA*.

Related commands

- [atmf virtual-link description](#)
- [atmf virtual-link protection](#)
- [show atmf](#)
- [show atmf links](#)
- [show atmf virtual-links](#)

Command changes Version 5.5.2-0.1: **remote-host** parameter added
Version 5.4.9-0.1: **interface** parameter added

atmf virtual-link description

Overview Use this command to add a description to an existing AMF virtual-link.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a description from an AMF virtual-link.

Syntax `atmf virtual-link id <1-4094> description <description>`
`no atmf virtual-link id <1-4094> description`

Parameter	Description
<code>id <1-4094></code>	ID of the local tunnel point.
<code><description></code>	A description for the virtual-link.

Default No description is set by default.

Mode Global Configuration

Example To add a description to the virtual-link with id '5', use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf virtual-link id 5 description T0 SITE B
```

To remove a description from the virtual-link with id '5', use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no atmf virtual-link id 5
```

Related commands [atmf virtual-link](#)
[show atmf links](#)
[show atmf virtual-links](#)

atmf virtual-link protection

Overview Use this command to add protection to an existing AMF virtual-link. Secure AMF virtual-links encapsulate the L2TPv3 frames of the virtual-link with IPsec.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove protection from an AMF virtual-link.

Syntax `atmf virtual-link id <1-4094> protection ipsec key [8] <key-string>`

`no atmf virtual-link id <1-4094> protection`

Parameter	Description
id	Specify the link ID.
	< Link ID in the range 1 to 4094
p	Protection is on for this link.
i	Security provided using IPsec.
k	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.
< s	Specify the shared key for the link.

Default Protection is off by default.

Mode Global Configuration

Usage notes Considered the following limitations when creating a secure virtual-link:

- Switch devices support a maximum of 20 downstream AMF nodes when using a secure virtual-link as an uplink.
- When there are two or more AMF members behind a shared NAT device, only one of the members will be able to use secure virtual-links.
- An AMF multi-tenant environment supports a maximum cumulative total of 1200 secure virtual-links across all AMF containers.

Example To create and configure a virtual link with protection, first create the virtual-link:

```
Host-A# configure terminal
```

```
Host-A(config)# atmf virtual-link id 1 ip 192.168.1.1 remote-id  
2 remote-ip 192.168.2.1
```

The enable protection on the virtual link:

```
Host-A(config)# atmf virtual-link id 1 protection ipsec key  
securepassword
```

Repeat these steps on the other side of the link:

```
Host-B(config)# atmf virtual-link id 2 ip 192.168.2.1 remote-id  
1 remote-ip 192.168.1.1
```

```
Host-B(config)# atmf virtual-link id 2 protection ipsec key  
securepassword
```

Related commands

- atmf virtual-link**
- show atmf**
- show atmf links**
- show atmf virtual-links**

Command changes Version 5.4.9-0.1: command added

atmf working-set

Overview Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

Use the **no** variant of this command to remove members or groups from the current working-set.

Syntax `atmf working-set { [<node-list> ] | [group {<group-list> | all | local | current}] }`
`no atmf working-set { [<node-list> ] | [group <group-list>] }`

Parameter	Description
<code><node-list></code>	A comma delimited list (without spaces) of nodes to be included in the working-set.
<code>group</code>	The AMF group.
<code><group-list></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 Running this command with the parameters group local 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)**.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
 - local: The originating node.
 - current: All nodes that comprise the current working-set.
 - all: All nodes in the AMF.
- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in **show atmf group** command output.

If a node is an AMF master it will be automatically added to the master group.

Example 1 To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf working-set group all
```

NOTE: This command adds the implicit group "all" to the working set, where "all" comprises all nodes in the AMF.

This command displays an output screen similar to the one shown below:

```
=====
node1, node2, node3, node4, node5, node6:
=====

Working set join

ATMF_NETWORK_Name[6]#
```

Example 2 To return to the local prompt, and connect to only the local node, use the command:

```
ATMF_Network_Name[6]# atmf working-set group local  
node1#
```

The following table describes the meaning of the prompts in this example.

Parameter	Description
ATMF_Network_Name	The name of the AMF network, as set by the atmf network-name .
[6]	The number of nodes in the working-set.
node1	The name of the local node, as set by the hostname .

bridge-group (amf-container)

Overview Use this command to connect an AMF container to a bridge created on a Virtual AMF Appliance (VAA) virtual machine for AMF Cloud. This allows the AMF container to connect to a physical network.

Note that this command is only available on AMF Cloud, not on AlliedWare Plus switches.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove a bridge-group from an AMF container.

Syntax bridge-group <bridge-id>
no bridge-group

Parameter	Description
<bridge-id>	The ID of the bridge group to join, a number between 1 and 64.

Mode AMF Container Configuration

Usage notes Each container has two virtual interfaces:

1. Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, and configured using this [area-link](#) command.
2. Interface eth1, used to connect to the outside world using a bridged L2 network link, and configured using the **bridge-group** command.

Before using this command, a bridge must be created with the same bridge-id on the VAA host using the **bridge <bridge-id>** command.

See the [AMF Feature Overview and Configuration Guide](#) for more information on configuring the bridge.

Example To assign a bridge group to AMF container 'vac-wlg-1', use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# bridge-group 1
```

Related **atmf container**
commands **show atmf container**

Command Version 5.4.7-0.1: command added
changes

clear application-proxy threat-protection

Overview Use this command to clear the threat protection for a specified address.

Syntax `clear application-proxy threat-protection {<ip-address>|<mac-address>|all}`

Parameter	Description
<ip-address>	The IPv4 address you wish to clear the threat for, in A.B.C.D format.
<mac-address>	The MAC address you wish to clear the threat for, in HHHH.HHHH.HHHH format.
all	Clear the threat for all IPv4 and MAC addresses.

Mode Privileged Exec

Example To clear the threat for 10.34.199.117, use the command:

```
awplus# clear application-proxy threat-protection 10.34.199.117
```

Related commands

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [application-proxy threat-protection send-summary](#)
- [service atm-application-proxy](#)
- [show application-proxy threat-protection](#)

Command changes Version 5.4.7-2.2: command added

clear atmf links

Overview Use this command with no parameters to manually reset all the AMF links on a device. You can optionally specify an interface or range of interfaces to reset the links on.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct, view of the network.

Syntax `clear atmf links [<interface-list>]`

Parameter	Description
<interface-list>	The interfaces or ports to perform the reset on. An interface-list can be: • a switchport (e.g. port1.0.1) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a local port (e.g. of0) • You can specify a continuous range of interfaces separated by a hyphen, or a comma-separated list (e.g. port1.0.1, port1.0.4-port1.0.18). The specified interfaces must exist. If this parameter is left out then all links of the specified type will be reset on the device.

Mode Privileged Exec

Example To clear all AMF links on a device, use the following command:

```
awplus# clear atmf links
```

To clear all AMF links on port1.0.1 to port1.0.4 and static aggregator sa1, use the following command:

```
awplus# clear atmf links port1.0.1-port1.0.4,sa1
```

Related commands [clear atmf links virtual](#)
[show atmf links](#)

Command changes Version 5.4.8-2.1: command added

clear atmf links virtual

Overview Use this command with no parameters to manually reset all the AMF virtual links on a device. You can, optionally, specify a comma separated list of virtual links to reset.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct view of the network.

Syntax `clear atmf links virtual [<virtuallink-list>]`

Parameter	Description
<virtuallink-list>	A single, or list, of AMF virtual link identifiers to reset. This must be a comma separated list of links e.g. <i>vlink1</i> , <i>vlink2</i> , <i>vlink3</i> . Specifying a link range e.g. <i>vlink1-vlink3</i> 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 The following shows typical output.

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><source-nodename></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
```

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'.

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><file-path URL></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
force	This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.
<source-name>	The filename and path of the source file. See the Introduction of the File and Configuration Management chapter for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction of the File and Configuration Management chapter for valid syntax.

Mode AMF Provisioning

Example To copy a configuration file named current.cfg from Node_4's Flash into the future_node directory, and set that configuration file to load onto future_node, use the following commands:

```
node_4# atmf provision node future_node
node_4(atmf-provision)# create
node_4(atmf-provision)# locate
node_4(atmf-provision)# copy flash:current.cfg ./future_node.cfg
node_4(atmf-provision)# configure boot config future_node.cfg
```

Related commands

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

Command changes Version 5.4.9-2.1: command added

create (amf-provision)

Overview This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command **clone (amf-provision)**.

This command can only run on AMF master nodes.

Syntax create

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

Example To create a new provisioned node named “device2” use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# create
```

Running this command will create the following directories:

- <media>:atmf/<atmf_name>/nodes/<node>
- <media>:atmf/<atmf_name>/nodes/<node>/flash

To confirm the new node’s settings, use the command:

```
device1# show atmf backup
```

The output for the **show atmf backup** command is shown in the following figure, and shows details for the new provisioned node ‘device2’.

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 variant of this command is .

Examples To enable all AMF debugging, use the command:

```
node_1# debug atmf
```

To enable AMF uplink and downlink debugging, use the command:

```
node_1# debug atmf link
```

To enable AMF error debugging, use the command:

```
node_1# debug atmf error
```

Related commands [no debug all](#)

debug atmf packet

Overview This command configures AMF Packet debugging parameters. The debug only displays information relevant to the current node. The command has following parameters:

Syntax debug atmf packet [direction {rx|tx|both}] [level {1|2|3}] [timeout <seconds>] [num-pkts <quantity>] [filter {node <name>| interface <ifname>} [pkt-type [1][2][3][4][5][6][7][8][9][10][11][12][13]]]

Simplified Syntax

debug atmf packet	[direction {rx tx both}]	
	[level {[1][2 3]}]	
	[timeout <seconds>]	
	[num-pkts <quantity>]	
debug atmf packet	filter	[node <name>]
		[interface <ifname>]
		[pkt-type [1][2][3][4][5][6][7][8][9][10][11][12][13]]

NOTE: You can combine the syntax components shown, but when doing so, you must retain their original order.

Default Level 1, both Tx and Rx, a timeout of 60 seconds with no filters applied.

NOTE: An alias to the variant of this command - - 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
<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.

Parameter	Description
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 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:

Sample output showing the show atmf backup command

```
device1#show atmf backup

Scheduled Backup ..... Enabled
  Schedule ..... 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2016 03:00
Backup Bandwidth ..... Unlimited
Backup Media ..... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .....
  Synchronization ..... Unsynchronized
    Last Run ..... -
    1 ..... Unconfigured
    2 ..... Unconfigured
Current Action ..... Idle
  Started ..... -
  Current Node ..... -
```

Node Name	Date	Time	In ATMF	On Media	Status
device1	30 Sep 2016	00:05:49	No	Yes	Good
device2	30 Sep 2016	00:05:44	Yes	Yes	Good

Related commands

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [identity \(amf-provision\)](#)
- [license-cert \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

Command changes Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

discovery

Overview Use this command to specify how AMF learns about guest nodes.

AMF nodes gather information about guest nodes by using one of the internally defined discovery methods: dynamic, static, or agent.

Dynamic learning (the default method) means that AMF learns the guest's IP and MAC addresses from LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6, use static learning.

Static learning uses the [switchport atmf-guestlink](#) command to specify the guest class name and IP address of the guest node attached to each individual switch port. AMF then learns the MAC addresses of each of the guests of that class from ARP or Neighbor discovery tables.

If you are using the static method, ensure that you have configured the appropriate class type for each of your statically discovered guest nodes.

Agent learning uses the AMF agent to retrieve the guest's IP and MAC address. It is only available on guest nodes that support ATMF agent, such as TQ5403 series access points. For step-by-step instructions on using agent discovery for auto-recovery of an TQ5403 series AP, see the [AMF Feature Overview and Configuration Guide](#).

The **no** variant of this command returns the discovery method to **dynamic**.

Syntax discovery [dynamic|static|agent]
no discovery

Parameter	Description
dynamic	Learned from DCHCP Snooping or LLDP.
static	Statically assigned.
agent	Learned from the AMF agent.

Default Dynamic

Mode AMF Guest Configuration

Usage notes This command is one of several modal commands that are configured and applied for a specific guest-class (mode). Its settings are automatically applied to a guest-node link by the [switchport atmf-guestlink](#) command.

NOTE: AMF guest nodes are not supported on ports using the OpenFlow protocol.

Example 1 To configure static discovery for the guest-class 'camera', use the following commands:

```
Node1# configure terminal

Node1(config)# atmf guest-class camera

Node1(config-atmf-guest)# discovery static
```

Example 2 To return the discovery method for the guest class TQ6602 to its default of **dynamic**, use the following commands:

```
Node1# configure terminal

Node1(config)# atmf guest-class TQ6602

Node1(config-atmf-guest)# no discovery
```

Related commands

- atmf guest-class**
- switchport atmf-guestlink**
- show atmf links guest**
- show atmf nodes**

Command changes Version 5.5.3-0.1: **agent** parameter added

description (amf-container)

Overview Use this command to set the description on an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove the description from an AMF container.

Syntax `description <description>`
`no description`

Parameter	Description
<code><description></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.
Note that you cannot use this command if you have **strict-user-process-control** enabled. Disable it before entering the **erase factory-default** command.

Example To erase data, use the command:

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

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

Related commands **atmf cleanup**

firmware-url

Overview Use this command to specify the location of an AP guest node's firmware file when preparing the AP for auto-recovery. AMF cannot back up AP firmware files (only configuration files), so you need to store the firmware file somewhere accessible and use this command to provide the AlliedWare Plus device with the file's location.

For step-by-step instructions for auto-recovery of an TQ5403 series AP, see the [AMF Feature Overview and Configuration Guide](#).

Use the **no** variant of this command to remove the URL.

Syntax `firmware-url <name>`
`no firmware-url`

Parameter	Description
<code><name></code>	The file's directory or filename. We recommend specifying a directory because that makes it easier to keep the firmware file up to date. The following protocols are supported: http, https, tftp, usb, and card. Do not change the firmware file's filename.

Default No URL is configured

Mode AMF Guest Configuration

Example To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored in the top level of a USB stick, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url usb:
```

To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored on a TFTP server with an address of 192.168.2.1, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url tftp://192.168.2.1/
```

Related commands **atmf guest-class**
discovery
login-fallback enable
modeltype
show atmf guests
show atmf guests detail
switchport atmf-guestlink

Command changes Version 5.5.3-0.1: command added

http-enable

Overview This command is used to enable GUI access to a guest node. When **http-enable** is configured, the port number is set to its default of 80. If the guest node is using a different port for HTTP, you can configure this using the **port** parameter.

This command is used to inform the GUI that this device has an HTTP interface at the specified port number so that a suitable URL can be provided to the user.

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

Syntax `http-enable [port <port-number>]`
`no http-enable`

Parameter	Description
port	TCP port number.
<port-number>	The port number to be configured.

Default Not set

Mode AMF Guest Configuration

Usage notes If **http-enable** is selected without a **port** parameter the port number will default to 80.

Example To enable HTTP access to a guest node on port 80 (the default), use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable
```

To enable HTTP access to a guest node on port 400, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable port 400
```

To disable HTTP access to a guest node, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# no http-enable
```

Related commands **atmf guest-class**
switchport atmf-guestlink
show atmf links guest
show atmf nodes

identity (amf-provision)

Overview Use this command to create an identity token for provisioning an isolated AMF node. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This command allows these nodes, which have no AMF neighbors, to be identified for provisioning purposes. They are identified using an identity token which is based on either the next-hop MAC address of the provisioned node, or the serial number of the device being provisioned. This identity token is stored on the AMF master.

Use the **no** variant of this command to remove the identity token for a node.

Syntax `identity mac-address <mac-address> prefix <ip-address/prefix-length>`
`identity serial-number <serial-number> prefix <ip-address/prefix-length>`
`no identity`

Parameter	Description
mac-address	Specify the next-hop MAC address of the device being provisioned.
<mac-address>	MAC address of the port the provisioned node is connected to, in the format xxxx.xxxx.xxxx.
serial-number	Specify the serial number of the device to be provisioned.
<serial-number>	Serial number of the device that is being provisioned.
prefix	IPv4 address, and prefix length, of the virtual-link interface on the isolated node
<ip-address/prefix-length>	IPv4 address, and prefix length, in A.B.C.D/M format.

Mode AMF Provisioning

Usage notes To provision an isolated node, first create a configuration for the node using the **create (amf-provision)** and/or the **clone (amf-provision)** commands.

Then create an identity token for the provisioned node by either specifying its next-hop MAC address or by specifying the serial number of the replacement device. The advantage of using the next-hop MAC address is that any device, regardless of its serial number, can be added to the network but using the serial number maybe preferred in situations where the next-hop MAC address is not easy to obtain.

The **atmf recovery-server** option must be enabled on the AMF master before attempting to provision the device. This option allows the AMF master to process recovery requests from isolated AMF nodes.

See the **AMF Feature Overview and Configuration Guide** for information on preparing your network for recovering or provisioning isolated nodes.

Example To create a identity token on your AMF master for a device named "my-x930" with serial number "A10064A172100008", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# identity serial-number A10064A172100008
prefix 192.168.2.25/24
```

To create a identity token on your AMF master for a device named "my-x930" with next-hop MAC address "0000.cd28.0880", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# identity mac-address 0000.cd28.0880
prefix 192.168.2.25/24
```

To delete the identity token from your AMF master for a device named "my-x930", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# no identity
```

Related commands

- atmf cleanup**
- atmf provision (interface)**
- atmf provision node**
- atmf recovery-server**
- atmf virtual-link**
- clone (amf-provision)**
- configure boot config (amf-provision)**
- configure boot system (amf-provision)**
- create (amf-provision)**
- delete (amf-provision)**
- license-cert (amf-provision)**
- locate (amf-provision)**
- show atmf provision nodes**

Command changes

- Version 5.4.9-0.1: syntax change due to new AMF provisioning mode
- Version 5.4.7-2.1: command added

license-cert (amf-provision)

Overview This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

Syntax license-cert <file-path|URL>
no license-cert

Parameter	Description
<file-path URL>	The name of the certificate file. This can include the file-path of the file.

Default No license certificate file is specified for the provisioned node.

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

Example 1 To apply the license certificate 'cert1.txt' stored on a TFTP server for AMF provisioned node "device2", use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# license-cert tftp://192.168.1.1/
cert1.txt
```

Example 2 To apply the license certificate 'cert2.txt' stored in the AMF master's flash directory for AMF provisioned node 'host2', use the command:

```
device1# atmf provision node host2
device1(atmf-provision)# license-cert /cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command **show atmf provision nodes**. The output from this command is shown below, and displays license certification details in the last line.

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.

Sample output from the pwd command

```
device2#pwd  
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

Related commands

- atmf provision (interface)**
- atmf provision node**
- clone (amf-provision)**
- configure boot config (amf-provision)**
- configure boot system (amf-provision)**
- copy (amf-provision)**
- create (amf-provision)**
- delete (amf-provision)**
- identity (amf-provision)**
- license-cert (amf-provision)**
- locate (amf-provision)**
- pwd**
- show atmf provision nodes**

Command changes Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

log event-host

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

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

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

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

Default Log events are disabled by default.

Mode Global Configuration

Usage notes Event hosts are set so syslog sends the messages out as they come.
Note that there is a difference between log event and log host messages:

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

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

```
Node1# configure terminal
```

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

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

```
Node1# configure terminal
```

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

Related commands [atmf topology-gui enable](#)

login-fallback enable

Overview Use this command to enable login fallback on TQ model AMF guest nodes. This allows AMF to try the factory default username and password if the guest node's saved username and password fail.

Use the **no** variant of this command to disable login fallback.

Syntax login-fallback enable
no login-fallback enable

Default Disabled

Mode AMF Guest Configuration

Usage notes This feature is only supported on TQ model guest nodes.

Login fallback means: if a guest node's saved username and password fail, AMF will try to connect to the node using the factory default username and password (manager/friend). When a new TQ replaces an existing TQ, this allows the new TQ to be discovered and managed as an AMF guest node. AMF can then start the AMF guest node recovery procedure.

Example To use the login fallback feature, first create an AMF guest class for TQ model APs. Then enable the login fall back feature.

For example, to enable login fallback on the guest-class AT-TQ5k, use the commands:

```
node1#configuration terminal
node1(config)#atmf guest-class AT-TQ5k
node1(config-atmf-guest)#login-fallback enable
node1(config-atmf-guest)#end
node1#
```

Related commands [atmf guest-class](#)
[modeltype](#)
[switchport atmf-guestlink](#)
[show atmf links guest](#)

Command changes Version 5.5.0-1.1: command added

modeltype

Overview This command sets the expected model type of the guest node. The model type will default to **other** if nothing is set.

Use the **no** variant of this command to reset the model type to **other**.

Syntax modeltype {alliedware|aw+|onvif|tq|other}
no modeltype

Parameter	Description
alliedware	A legacy Allied Telesis operating system.
aw+	The Allied Telesis AlliedWare Plus operating system.
onvif	ONVIF (Open Network Video Interface Forum) Profile Q devices
tq	An Allied Telesis TQ Series wireless access point.
other	Used where the model type is outside the above definitions.

Default Default to **other**

Mode AMF Guest Configuration

Examples To assign the model type **tq** to the guest-class called 'tq_device', use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-vmf-guest)# modeltype tq
```

To remove the model type **tq** from the guest-class called 'tq_device', and reset it to the default of **other**, use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-vmf-guest)# no modeltype
```

Related commands [atmf guest-class](#)
[switchport atmf-guestlink](#)
[show atmf links guest](#)

Command changes Version 5.4.9-2.1: **onvif** parameter added

service atmf-application-proxy

Overview Use this command to enable the AMF Application Proxy service. This service distributes messages across all AMF nodes.

Currently this is used for threat protection. When an AMF Security (AMF-Sec) Controller detects a threat, it issues a request to block the address the threat originated from. The AMF Application Proxy service distributes this message to all AMF nodes. An AMF master accepts this block request and instructs the subordinate AMF node to block the relevant device.

Use the **no** variant of this command to disable the AMF Application Proxy service.

Syntax service atmf-application-proxy
no service atmf-application-proxy

Default The AMF Application Proxy service is disabled by default.

Mode Global Configuration

Usage notes The AMF master maintains a list of all threats and will send this list to any AMF node, or VCS member, when it boots and joins the AMF network.

In order for this to work the follow must be configured:

- the AMF Application Proxy service on all AMF nodes that need to receive the messages.
- the Hypertext Transfer Protocol (HTTP) service on all nodes that are running the AMF Application Proxy service (see [service http](#)).

Example To enable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# service atmf-application-proxy
```

To disable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# no service atmf-application-proxy
```

Related commands [application-proxy threat-protection](#)
[application-proxy whitelist server](#)
[clear application-proxy threat-protection](#)
[show application-proxy threat-protection](#)

Command changes Version 5.4.7-2.2: command added

show application-proxy threat-protection

Overview Use this command to list all the IP addresses blocked by the AMF Application Proxy service. It also shows the global threat-detection configuration.

Syntax show application-proxy threat-protection [all]

Parameter	Description
all	Include information for non-local blocks.

Mode Privileged Exec

Example To list the addresses blocked by the AMF Application Proxy service, use the command:

```
awplus# show application-proxy threat-protection
```

Output The following shows typical output.

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
...
```

Parameters in the output from show application-proxy threat-protection

Parameter	Description
Quarantine Vlan	The name of the quarantine VLAN.
Global IP-Filter	The status of global IP filtering.
IP-Filter Limit Exceeded	The number of times an ACL failed to be installed due to insufficient space.
Redirect-URL	The URL a blocked user is redirected to.

Related commands [application-proxy quarantine-vlan](#)
[application-proxy threat-protection](#)
[clear application-proxy threat-protection](#)
[service atmf-application-proxy](#)

Command changes Version 5.4.7-2.2: command added

show application-proxy whitelist advertised-address

Overview Use this command to show the Layer 3 interface and its IPv4 address that is advertised as the application-proxy whitelist address.

Syntax show application-proxy whitelist advertised-address

Mode Privileged Exec

Example To display the interface and IPv4 address advertised as the application-proxy whitelist address, use the command:

```
awplus# show application-proxy whitelist advertised-address
```

Output The following shows typical output.

Example output from show application-proxy whitelist advertised-address

```
awplus#show application-proxy whitelist advertised-address
ATMF Application Proxy Whitelist advertised-address:
  Interface   : vlan1001
  IP address  : 10.34.16.5
```

Related commands [application-proxy whitelist advertised-address](#)
[application-proxy whitelist server](#)

Command changes Version 5.4.9-1.1: command added

show application-proxy whitelist interface

Overview Use this command to display the status of port authentication on the specified interface.

Syntax show application-proxy whitelist interface [*<interface-list>*]

Parameter	Description
<i><interface-list></i>	The interfaces or ports to display information about. An interface-list can be: • a switchport (e.g. port1.0.4) • a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4) • a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list. The specified interface must exist.

Mode Privileged Exec

Example To display the port authentication information for all interfaces, use the command:

```
awplus# show application-proxy whitelist interface
```

To display the port authentication information for port1.0.4, use the command

```
awplus# show application-proxy whitelist interface port1.0.4
```

Output The following shows typical output.

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 The following shows typical output.

Example output from show application-proxy whitelist server

```
awplus#show application-proxy whitelist server
Application Proxy Whitelist Details:
External Server Details:
  IP: 192.168.1.10
  Port: 2083
  Protection: TLS
  Trustpoint: None (Authentication disabled)
Proxy Details:
  IP: 172.31.0.5
  Status: Alive
```

Related commands [application-proxy whitelist enable](#)
[application-proxy whitelist server](#)
[show application-proxy whitelist interface](#)
[show application-proxy whitelist supplicant](#)

Command changes Version 5.4.9-0.1: command added

show application-proxy whitelist supplicant

Overview Use this command to display the current configuration and status for each supplicant attached to an application-proxy whitelist port.

Syntax show application-proxy whitelist supplicant [interface <interface-list>|<mac-addr>|brief]

Parameter	Description
interface <interface-list>	The interfaces or ports to display information about. An interface-list can be: • a switchport (e.g. port1.0.4) • a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4) • a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list. The specified interface must exist.
<mac-addr>	MAC (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal)
brief	Brief summary of the supplicant state.

Mode Privileged Exec

Example To display the supplicant information for all ports, use the command:

```
awplus# show application-proxy whitelist supplicant
```

To display the supplicant information for port1.0.4, use the command:

```
awplus# show application-proxy whitelist supplicant  
interface port1.0.4
```

Output The following shows typical output.

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
```

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.

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
```

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
```

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.
Node Name	The name assigned to a particular node.

Parameter	Definition
Role	The role configured for this AMF device, either Master or Member.
Current ATMF Nodes	The count of AMF nodes in an AMF Network.
Node Address	An address used to access a remotely located node (.atmf).
Node ID	A unique identifier assigned to a Node on an AMF network.
Node Depth	The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
Domain State	The state of Node in a Domain in AMF network as Controller/Backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between Nodes of different domain (up/down links). - VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. - Management Subnet - Network prefix for the subnet. - Management IP Address - The IP address allocated for this traffic. - Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). - VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. - Domain Subnet. The subnet address used for this traffic. - Domain IP Address. The IP address allocated for this traffic. - Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
Device Type	The Product Series name.
ATMF Master	Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).
SC	The device configuration, one of C - Chassis (SBx8100 Series), S - Stackable (VCS) or N - Standalone.
Parent	The node to which the current node has an active uplink.
Node Depth	The number of nodes in the path from this node to the master node.

Related commands [show atmf detail](#)

show atmf area

Overview Use this command to display information about an AMF area. On AMF controllers, this command displays all areas that the controller is aware of. On remote AMF masters, this command displays the controller area and the remote local area. On gateways, this command displays the controller area and remote master area.

Syntax show atmf area [detail] [<area-name>]

Parameter	Description
detail	Displays detailed information
<area-name>	Displays information about master and gateway nodes in the specified area only.

Mode Privileged Exec

Example 1 To show information about all areas, use the command:

```
controller-1# show atmf area
```

The following figure shows example output from running this command on a controller.

Example output from the show atmf area command on a Controller.

```
controller-1#show atmf area
```

ATMF Area Information:

* = Local area

Area Name	Area ID	Local Gateway	Remote Gateway	Remote Master	Node Count
* NZ	1	Reachable	N/A	N/A	3
Wellington	2	Reachable	Reachable	Auth OK	120
Canterbury	3	Reachable	Reachable	Auth Error	-
SiteA-AREA	14	Unreachable	Unreachable	Unreachable	-
Auckland	100	Reachable	Reachable	Auth Start	-
Southland	120	Reachable	Reachable	Auth OK	54
Area count:	6			Area node count:	177

The following figure shows example output from running this command on a remote master.

Example output from the show atmf area command on a remote master.

```
Canterbury#show atmf area
```

ATMF Area Information:

* = Local area

Area Name	Area ID	Local Gateway	Remote Gateway	Remote Master	Node Count
NZ	1	Reachable	N/A	N/A	-
* Canterbury	3	Reachable	N/A	N/A	40
Area count:	2			Local area node count:	40

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:

Parameter	Definition
	• Reachable, if the link has been established. • Unreachable, if a link to the remote area has not been established. This could mean that a port or vlan is down, or that inconsistent VLANs have been configured using the switchport atmf-arealink command. • N/A for the area of the controller or remote master on which the command is being run, because the gateway node on that device is local. • Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match. • Auth Error, which indicates that the areas tried to authenticate but there is a problem. For example, the passwords configured on the controller and remote master may not match, or a password may be missing on the remote master.# • Auth OK, which indicates that area authentication was successful and you can now use the atmf select-area command.
Remote Master	Whether the remote master node is reachable or not. This is N/A for the area of the controller or remote master on which the command is being run, because the master node on that device is local.
Node Count	The number of nodes in the area.
Area Count	The number of areas controlled by the controller.
Area Node Count	The total number of nodes in the area.

Example 2 To show detailed information about the areas, use the command:

```
controller-1# show atmf area detail
```

The following figure shows example output from running this command.

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><area-name></i>	The area name for guest information
<i><node-name></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 The following shows typical output.

Example output from the show atmf area guests command

main-building Area Guest Node Information:				
Device Type	MAC Address	Parent	Port	IP/IPv6 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]#				

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><area-name></i>	The name assigned to the AMF area. An area is an AMF network that is under the control of an AMF Controller.
<i><node-name></i>	The name assigned to the network node.

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 The following shows typical output.

Example output from the show atmf guest detail command.

```
#show atmf guest detail

Node Name           : Node1
Port Name           : port1.0.5
Ifindex             : 5005
Guest Description    : tq4600
Device Type         : AT-TQ4600
Configuration Mismatch : No
Backup Supported     : Yes
MAC Address         : eccd.6df2.da60
IP Address          : 192.168.4.50
IPv6 Address        : Not Set
HTTP Port           : 80
Firmware Version    :

Node Name           : poe
Port Name           : port1.0.6
Ifindex             : 5006
Guest Description    : tq3600
Device Type         : AT-TQ2450
Configuration Mismatch : No
Backup Supported     : Yes
MAC Address         : 001a.eb3b.cb80
IP Address          : 192.168.4.9
IPv6 Address        : Not Set
HTTP Port           : 80
Firmware Version    :
```

Parameters shown in the output of the show atmf guest detail command

Parameter	Description
Node Name	The name of the guest's parent node.
Port Name	The port on the parent node that connects to the guest.
Ifindex	An internal index number that maps to the port number on the parent node.
Guest Description	A brief description of the guest node as manually entered into the description (interface) command for the guest node port on the parent node.
Device Type	The device type as supplied by the guest node itself.
Backup Supported	Indicates whether AMF supports backup of this guest node.
MAC Address	The MAC address of the guest node.
IP Address	The IP address of the guest node.
IPv6 Address	The IPv6 address of the guest node.
HTTP Port	The HTTP port enables you to specify a port when enabling http to allow a URL for the http user

Parameter	Description
	interface of a Guest Node. This is determined by the http-enable command.
Firmware Version	The firmware version that the guest node is currently running.

Related commands **show atmf area nodes-detail**
show atmf area guests

show atmf area nodes

Overview Use this command to display summarized information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax show atmf area nodes *<area-name>* [*<node-name>*]

Parameter	Description
<i><area-name></i>	Displays information about nodes in the specified area.
<i><node-name></i>	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.

Output from the show atmf area nodes wellington command

```
controller-1#show atmf area nodes wellington
```

Wellington Area Node Information:					
Node Name	Device Type	ATMF Master	SC	Parent Domain	Node Depth
well-gate	x230-18GP	N	N	well-master	1
well-master	AT-x930-28GPX	Y	N	none	0

Wellington node count 2

Parameter definitions from the show atmf area nodes command

Parameter	Definition
Node Name	The name assigned to a particular node.
Device Type	The Product series name.
ATMF Master	Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).
SC	The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone.
Parent Domain	The node to which the current node has an active uplink.
Node Depth	The number of nodes in the path from this node to the master node.

Related commands [show atmf area](#)
[show atmf area nodes-detail](#)

show atmf area nodes-detail

Overview Use this command to display detailed information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax `show atmf area nodes-detail <area-name> [<node-name>]`

Parameter	Description
<code><area-name></code>	Displays detailed information about nodes in the specified area.
<code><node-name></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.

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

...
```

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
<i><area-name></i>	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.

Output from the show atmf area summary command

```
controller-1#show atmf area summary

ATMF Area Summary Information:

Management Information
  Local IPv6 Address           : fd00:4154:4d46:1::15

Area Information
  Area Name                   : NZ (Local)
  Area ID                     : 1
  Area Master IPv6 Address    : -

  Area Name                   : Wellington
  Area ID                     : 2
  Area Master IPv6 Address    : fd00:4154:4d46:2::149

  Area Name                   : Canterbury
  Area ID                     : 3
  Area Master IPv6 Address    : fd00:4154:4d46:3::f

  Area Name                   : Auckland
  Area ID                     : 100
  Area Master IPv6 Address    : fd00:4154:4d46:64::17
  Interface                   : vlink2000
```

Related commands

- [show atmf area](#)
- [show atmf area nodes](#)
- [show atmf area nodes-detail](#)

show atmf authorization

Overview Use this command on an AMF master to display the authorization status of other AMF members and masters on the network.

On an AMF controller this command will show the authorization status of remote area AMF masters.

Syntax `show atmf authorization {current|pending|provisional}`

Parameter	Description
current	Show the status of all authorized nodes.
pending	Show the status of unauthorized nodes in the pending queue. These are nodes that enabled secure mode with atmf secure-mode but have not yet been authorized with atmf authorize .
provisional	Show the status of provisionally authorized nodes. These are nodes that have been provisioned with atmf authorize provision .

Mode Privileged Exec

Example To display all authorized AMF nodes on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization current
```

To display AMF nodes which are requesting authorization on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization pending
```

To display AMF nodes which have provisional authorization, use the command:

```
awplus# show atmf authorization provisional
```

Output The following shows typical output.

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

Parameters in the output from show atmf authorization current

Parameter	Description
Node Name	AMF node name of the authorized node.
Signer	Name of the AMF master that authorized the node.
Expires	Expiry date of the authorization. Authorization expiry time is set using atmf secure-mode certificate expiry .

Output The following shows typical output.

Example output from show atmf authorization pending

Pending Authorizations:			
NZ Requests:			
Node Name	Product	Parent Node	Interface

area_1_node_3	x230-18GP	master_1	port1.2.9
area_1_node_4	x510-52GTX	master_1	sa1

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 The following shows typical output.

Example output from show atmf authorization provisional

ATMF Provisional Authorization:			
Area - Node Name or MAC Address	Interface	Start Time	Timeout 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

Parameters in the output from show atmf authorization provisional

Parameter	Description
Area - Node Name or MAC Address	MAC address or node name of the node that has been provisionally authorized.
Interface	Interface that the node has been provisioned on.
Start Time	Time the node was provisioned.
Timeout Minutes	Length of time from Start Time until the provisional authorization expires.

Related commands

- [atmf authorize](#)
- [atmf authorize provision](#)
- [atmf secure-mode](#)
- [clear atmf secure-mode certificates](#)
- [show atmf](#)
- [show atmf secure-mode](#)
- [show atmf secure-mode certificates](#)

Command changes Version 5.4.7-0.3: command added

show atmf backup

Overview This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

Syntax show atmf backup
show atmf backup logs
show atmf backup server-status
show atmf backup synchronize [logs]

Parameter	Description
logs	Displays detailed log information.
server-status	Displays connectivity diagnostics information for each configured remote file server.
synchronize	Display the file server synchronization status
logs	For each remote file server, display the logs for the last synchronization

Mode Privileged Exec

Example 1 To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

To display log messages to do with backups, use the command:

```
node_1# show atmf backup logs
```

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

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
```

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
```

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
```

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).
Status	The output can contain one of four values: • “-” meaning that the status file cannot be found or cannot be read. • “Errors” meaning that there are issues - note that the backup may still be deemed successful depending on the errors. • “Stopped” meaning that the backup attempt was manually aborted. • “Good” meaning that the backup was completed successfully. • “In Progress” meaning that the backup is currently running on that node.

Parameter	Definition
Log File Location	All backup attempts will generate a result log file in the identified directory based on the node name. In the above example this would be: card:/amf/office/logs/rsync_amf_testbox1.log.
Log Details	The contents of the backup log file.
server-status	Displays connectivity diagnostics information for each configured remove file server.

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

Related commands [show atmf](#)
[atmf network-name](#)

show atmf backup area

Overview Use this command to display backup status information for the master nodes in one or more areas.

Note that this command is only available on AMF controllers.

Syntax show atmf backup area [*<area-name>*] [*<node-name>*] [logs]

Parameter	Description
logs	Displays the logs for the last backup of each node.
<i><area-name></i>	Displays information about nodes in the specified area.
<i><node-name></i>	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
```

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-area link

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
<code><node-name></code>	The name of parent guest node
<code><guest-port></code>	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 The following shows typical output.

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
```

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 The following shows typical output.

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
```

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
```

Parameters in the output from show atmf container

Parameter	Description
Container	Name of the AMF container.
Area	Name of the area the container is in.
Bridge	Name of the bridge connecting the container to the physical network.
State	Container state, running or stopped. This is set with the state command.
Memory	The amount of memory the container is using on the VAA host.
CPU%	The percentage of CPU time the container is using on the VAA, at the time the show command is run.

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
```

Parameters in the output from show atmf container detail

Parameter	Description
Name	Name of the AMF container.
State	Container state, RUNNING or STOPPED. This is set with the state command.
PID	Internal container id.
IP	This lists the IP addresses used by the container. These include the eth1 IP address and the AMF management IP address.
CPU use	The CPU usage of the container since it was enabled.
Memory use	Container memory usage.
Link	Each container has two links: 1. An AMF area-link, this connects the container to the AMF controller and uses virtual interface eth0 on the AMF container. 2. A bridged L2 network link, this connects the container to the outside world and uses the virtual interface eth1 on the AMF container. See the AMF Feature Overview and Configuration_Guide for more information on these links.
TX/RX bytes	Bytes sent and received on a link.
Total bytes	Total bytes transferred on a link.

Related commands

- [area-link](#)
- [atmf area](#)
- [atmf area password](#)
- [atmf container](#)
- [atmf container login](#)
- [bridge-group \(amf-container\)](#)
- [description \(amf-container\)](#)
- [state](#)

Command changes Version 5.4.7-0.1: command added

show atmf detail

Overview This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

Syntax show atmf detail

Parameter	Description
detail	Displays output in greater depth.

Mode Privileged Exec

Example 1 To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
atmf-1#show atmf detail
ATMF Detail Information:

Network Name           : Test_network
Network Mtu            : 1300
Node Name              : controller-1
Node Address           : controller-1.atmf
Node ID                : 342
Node Depth             : 0
Domain State           : BackupDomainController
Recovery State         : None
Recovery Over ETH Ports : Disabled
Log Verbose Setting    : Verbose
Topology GUI           : Disabled

Management VLAN
VLAN ID                : 4000
Management Subnet      : 172.31.0.0
Management IP Address  : 172.31.1.86
Management Mask        : 255.255.128.0
Management IPv6 Address : fd00:4154:4d46:1::156
Management IPv6 Prefix Length : 64

Domain VLAN
VLAN ID                : 4091
Domain Subnet          : 172.31.128.0
Domain IP Address      : 172.31.129.86
Domain Mask            : 255.255.128.0
```

Parameter definitions from the show atmf detail command

Parameter	Definition
Network MTU	The network MTU for the ATMF network.
Network Name	The AMF network that a particular node belongs to.
Node Name	The name assigned to a particular node.
Node Address	An address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).
Node ID	A unique identifier assigned to a node on an AMF network.
Node Depth	The number of nodes in the path from this node to the level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
Domain State	The state of a node in a Domain in an AMF network as Controller/Backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.

Parameter	Definition
Recovery Over ETH Ports	Allow AMF recovery over the Eth port on an AR-series device.
Log Verbose Setting	The state of the atmf log-verbose command.
Topology GUI	This feature allows your AMF network to interact with Vista Manager EX and must be enabled on your AMF master.
Management VLAN	The VLAN created for traffic between nodes of different domain (up/down links). • VLAN ID - in this example VLAN 4092 is configured as the Management VLAN. • Management Subnet - the network prefix for the subnet. • Management IP Address - the IP address allocated for this traffic. • Management Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).
Domain VLAN	The VLAN assigned for traffic between nodes of the same domain (crosslink). • VLAN ID - in this example VLAN 4091 is configured as the domain VLAN. • Domain Subnet - the subnet address used for this traffic. • Domain IP Address - the IP address allocated for this traffic. • Domain Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).
Node Depth	The number of nodes in the path from this node to the core domain.

show atmf group

Overview This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

Syntax `show atmf group [user-defined|automatic]`

Parameter	Description
user-defined	User-defined-group information display.
automatic	Automatic group information display.

Default All groups are displayed

Mode Privileged Exec

Example 1 To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information
master, x510
node2#
```

This screen shows that node2 contains the groups **master** and **x510**. Note that although the node also contains the implicit groups, these do not appear in the show output.

Example 2 The following commands (entered on *node2*) will display all the automatic groups within the working set containing *node1* and all nodes that have been pre-defined to contain the *sysadmin* group:

First define the working-set:

```
node1# #atmf working-set node1 group sysadmin
```

A typical output screen from this command is shown below:

```
ATMF group information
master, poe, x8100

=====
node1, node2, node3, node4, node5, node6:
=====

ATMF group information
sysadmin, x8100
AMF_NETWORK[6]#
```

This confirms that the six nodes (*node1* to *node6*) are now members of the working-set and that these nodes reside within the *AMF-NETWORK*.

Note that to run this command, you must have previously entered the command **atmf working-set**. This can be seen from the network level prompt, which in this case is *AMF_NETWORK[6]#*.

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
```

Parameter definitions from the show atmf group command for a working set

Parameter	Definition
ATMF group information	Displays a list of nodes and the groups that they belong to, for example: • master - Shows a common group name for Nodes configured as AMF masters. • Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x230, for example. • User-defined - Arbitrary groups created by the user for AMF nodes.

show atmf group members

Overview This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

Syntax show atmf group members [user-defined|automatic]

Parameter	Description
user-defined	User defined group membership display.
automatic	Automatic group membership display.

Mode Privileged Exec

Example To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

Sample output from the show atmf group members command

ATMF Group membership		
Automatic Groups	Total Members	Members

master	1	Building_1
poe	1	HW_Team1
x510	3	SW_Team1 SW_Team2 SW_Team3
x930	1	HW_Team1
x8100	2	Building_1 Building_2
ATMF Group membership		
User-defined Groups	Total Members	Members

marketing	1	Bld1_Floor_1
software	3	SW_Team1 SW_Team2 SW_Team3

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 The following shows typical output.

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
```

Parameters shown in the output of the show atmf guests command

Parameter	Description
Device Name	The name that is discovered from the device, or failing that, a name that is auto-assigned by AMF. The auto-assigned name consists of:<parent node name>-<attached port number>You can change this by configuring a description on the port.
Device Type	The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the atmf guest-class command.
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><node-name></code>	The name of the guest node's parent.
<code><guest-port></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 The following shows typical output.

Example output from show atmf guests detail

```
master#show atmf guests detail

ATMF Guest Node Information:

Node Name           : master
Port Name           : port1.0.9
Ifindex             : 5009
Guest Description    : red-1.0.9
Device Type         : x600-24Ts
Backup Supported     : No
MAC Address         : 0000.cd38.0c4d
IP Address          : 192.168.1.5
IPv6 Address        : Not Set
HTTP Port           : 0
Firmware Version    : 5.4.2-0.1

Node Name           : node1
Port Name           : port1.0.13
Ifindex             : 5013
Guest Description    : node1-1.0.13
Device Type         : AT-TQ4600
Backup Supported     : Yes
MAC Address         : eccd.6df2.daa0
IP Address          : 192.168.5.6
IPv6 Address        : Not Set
HTTP Port           : 80
Firmware Version    : 3.1.0 B01
```

Parameters in the output from show atmf guests detail.

Parameter	Description
Node Name	The name of the parent node, which is the AMF node that directly connects to the guest node.
Port Name	The port on the parent node that connects to the guest.
IfIndex	An internal index number that maps to the port number on the parent node.
Guest Description	A description that is discovered from the device, or failing that, auto-assigned by AMF. The auto-assigned name consists of: <parent node name>-<attached port number>. You can change this by configuring a description on the port.
Device Type	The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the atmf guest-class command.
Username	The user name configured on the guest node.
Backup Supported	Whether the guest node supports AMF backup functionality.

Parameter	Description
MAC Address	The MAC address of the guest node.
IP Address	The IP address of the guest node.
IPv6 Address	The IPv6 address of the guest node.
Firmware Version	The version of the firmware operating on the guest node.
HTTP port	The HTTP port as specified with the http-enable command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).

Related commands [atmf guest-class](#)
[switchport atmf-guestlink](#)
[show atmf backup guest](#)

show atmf links

Overview This command displays information about AMF links on a switch. The display output contains link status state information.

Syntax show atmf links [brief]

Parameter	Description
brief	A brief summary of AMF links, their configuration and status.

Mode User Exec and Privileged Exec

Usage notes The **show atmf links** and **show atmf links brief** commands both produce a table of summarized link information. For a more detailed view use the **show atmf links detail** command.

This command does not show links that are configured on provisioned ports.

Example To display a brief summary of the AMF links, use the following command:

```
node-1# show atmf links brief
```

Example output from show atmf links brief

Example-core# show atmf links						
ATMF Link Brief Information:						
Local Port	Link Type	Link Status	ATMF State	Adjacent Node	Adjacent Ifindex	Link 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.						

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.
ATMF State	Shows AMF state of the local port: • Init - Link is down. • Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. • Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. • OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain. • OneWaySim - Device is running in secure mode and link is up but waiting for authorization from an AMF master. • Full - Link hello packets are sent and received from its neighbor with its own node id. • Shutdown - Link has been shut down by user configuration.
Adjacent Node	Shows the Adjacent AMF Node to the one being configured.
Adjacent IF Index	Shows the IF index for the Adjacent AMF Node connected to the node being configured.
Link State	Shows the state of the AMF link. Valid states are either Forwarding or Blocking.

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

Related commands

- [no debug all](#)**
- [clear atmf links statistics](#)**
- [show atmf](#)**
- [show atmf links detail](#)**
- [show atmf links guest](#)**
- [show atmf links guest detail](#)**
- [show atmf links statistics](#)**
- [show atmf nodes](#)**

show atmf links detail

Overview This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

Syntax show atmf links detail

Parameter	Description
detail	Detailed AMF links information.

Mode User Exec

Usage notes For summarized link information see the [show atmf links](#) command. This command does not show links that are configured on provisioned ports.

Example To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links. The following example gives details of the links that are summarized in the example in [show atmf links](#).

Sample output from the show atmf links detail command

```
device1# show atmf links detail

-----
Crosslink Ports Information
-----
Port                : sa1
Ifindex             : 4501
Port Status         : Down
Port State          : Init
Last event          :
Port BPDU Receive Count : 0

Port                : po10
Ifindex             : 4610
Port Status         : Up
Port State          : Full
Last event          : AdjNodeLSEPresent
Port BPDU Receive Count : 140
Adjacent Node Name  : Building-B
Adjacent Ifindex    : 4610
Adjacent MAC        : eccd.6dd1.64d0
Port Last Message Response : 0

Port                : po30
Ifindex             : 4630
Port Status         : Up
Port State          : Full
Last event          : AdjNodeLSEPresent
Port BPDU Receive Count : 132
Adjacent Node Name  : Building-A
Adjacent Ifindex    : 4630
Adjacent MAC        : eccd.6daa.c861
Port Last Message Response : 0

Link State Entries:

Crosslink Ports Blocking : False
Node.Ifindex             : Building-A.4630 - Example-core.4630
Transaction ID           : 2 - 2
MAC Address              : eccd.6daa.c861 - 0000.cd37.054b
Link State               : Full - Full

Node.Ifindex             : Building-B.4610 - Example-core.4610
Transaction ID           : 2 - 2
MAC Address              : eccd.6dd1.64d0 - 0000.cd37.054b
Link State               : Full - Full

Domain Nodes Tree:

Node                     : Building-A
  Links on Node          : 1
  Link 0                 : Building-A.4630 - Example-core.4630
  Forwarding State       : Forwarding
Node                     : Building-B
  Links on Node          : 1
  Link 0                 : Building-B.4610 - Example-core.4610
  Forwarding State       : Forwarding
Node                     : Example-core
  Links on Node          : 2
```

```

Link 0                : Building-A.4630 - Example-core.4630
Forwarding State      : Forwarding
Link 1                : Building-B.4610 - Example-core.4610
Forwarding State      : Forwarding

Crosslink Transaction Entries:

Node                  : Building-B
Transaction ID        : 2
Uplink Transaction ID : 6
Node                  : Building-A
Transaction ID        : 2
Uplink Transaction ID : 6

Uplink Information:

Waiting for Sync      : 0
Transaction ID        : 6
Number of Links       : 0
Number of Local Uplinks : 0

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

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

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

```

Parameter definitions from the show atmf links detail command output

Parameter	Definition
Crosslink Ports Information	Show details of all Crosslink ports on this Node: - Port - Name of the Port or static aggregation (sa<*>). - Ifindex - Interface index for the crosslink port. - VR ID - Virtual router id for the crosslink port. - Port Status - Status of the local port on the Node as UP or DOWN. - Port State - AMF State of the local port. - Init - Link is down. - Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. - Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. - OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain - Full - Link hello packets are sent and received from its neighbor with its own node id. - Shutdown - Link has been shut down by user configuration. Port BPDU Receive Count - The number of AMF protocol PDU's received. - Adjacent Node Name - The name of the adjacent node connected to this node. - Adjacent Ifindex - Adjacent AMF Node connected to this Node. - Adjacent VR ID - Virtual router id of the adjacent node in the domain. - Adjacent MAC - MAC address of the adjacent node in the domain. - Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.

Parameter	Definition
Link State Entries	Shows all the link state database entries: • Node.Ifindex - Shows adjacent Node names and Interface index. • Transaction ID - Shows transaction id of the current crosslink transaction. • MAC Address - Shows adjacent Node MAC addresses. • Link State - Shows AMF states of adjacent nodes on the link.
Domain Nodes Tree	Shows all the nodes in the domain: • Node - Name of the node in the domain. • Links on Node - Number of crosslinks on a vertex/node. • Link no - Shows adjacent Node names and Interface index. • Forwarding State - Shows state of AMF link Forwarding/Blocking.
Crosslink Transaction Entries	Shows all the transaction entries: • Node - Name of the AMF node. • Transaction ID - transaction id of the node. • Uplink Transaction ID - transaction id of the remote node.
Uplink Information	Show all uplink entries. • Waiting for Sync - Flag if uplinks are currently waiting for synchronization. • Transaction ID - Shows transaction id of the local node. • Number of Links - Number of up downlinks in the domain. • Number of Local Uplinks - Number of uplinks on this node to the parent domain. • Originating Node - Node originating the uplink information. • Domain - Name of the parent uplink domain. • Node - Name of the node in the parent domain, that is connected to the current domain. • Ifindex - Interface index of the parent node's link to the current domain. • VR ID - Virtual router id of the parent node's link to the current domain. • Transaction ID - Transaction identifier for the neighbor in crosslink. • Flags - Used in domain messages to exchange the state: - ATMF_DOMAIN_FLAG_DOWN = 0 - ATMF_DOMAIN_FLAG_UP = 1 - ATMF_DOMAIN_FLAG_BLOCK = 2 - ATMF_DOMAIN_FLAG_NOT_PRESENT = 4 - ATMF_DOMAIN_FLAG_NO_NODE = 8 - ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16 - ATMF_DOMAIN_FLAG_NOT_LINKS = 32 - ATMF_DOMAIN_FLAG_NO_CONFIG = 64 • Domain Controller - Domain Controller in the uplink domain

Parameter	Definition
	Domain Controller MAC - MAC address of Domain Controller in uplink domain
Downlink Domain Information	Shows all the downlink entries: - Domain - Name of the downlink domain. - Domain Controller - Controller of the downlink domain. - Domain Controller MAC - MAC address of the domain controller. - Number of Links - Total number of links to this domain from the Node. - Number of Links Up - Total number of links that are in UP state. - Number of Links on This Node - Number of links terminating on this node. - Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.
Node Transaction List	List of transactions from this downlink domain node. - Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain. - Transaction ID - Transaction id for this node. - Domain List: Shows list of nodes in the current domain and their links to the downlink domain.: - Domain - Domain name of the downlink node. - Node - Name of the node in the current domain. - Ifindex - Interface index for the link from the node to the downlink domain. - Transaction ID - Transaction id of the node in the current domain. - Flags - As mentioned above.
Up/Downlink Ports Information	Shows all the configured up and down link ports on this node: - Port - Name of the local port. - Ifindex - Interface index of the local port. - VR ID - Virtual router id for the local port. - Port Status - Shows status of the local port on the Node as UP/DOWN. - Port State - AMF state of the local port. - Adjacent Node - nodename of the adjacent node. - Adjacent Internal ID - Unique node identifier of the remote node. - Adjacent Ifindex - Interface index for the port of adjacent AMF node. - Adjacent Board ID - Product identifier for the adjacent node. - Adjacent VR ID - Virtual router id for the port on adjacent AMF node. - Adjacent MAC - MAC address for the port on adjacent AMF node. - Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node. - Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node. - Port Forwarding State - Local port forwarding state Forwarding or Blocking. - Port BPDU Receive Count - count of AMF protocol PDU's received.

Parameter	Definition
	• Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes. • Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived. • Port Last Message Response - response from the remote neighbor to our last hello packet.

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

Related commands **no debug all**
clear atmf links statistics
show atmf

show atmf links guest

Overview This command displays information about guest nodes visible to an AMF device.

Syntax show atmf links guest [interface <interface-range>]

Parameter	Description
interface <interface-range>	Select a specific range of ports to display information about guest nodes.

Default With no parameters specified this command will display its standard output for all ports with guest nodes connected.

Mode User Exec/Privileged Exec

Usage notes Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests](#).

Example 1 To display information about AMF guests that are connectible from node1, use the command:

```
node1# show atmf links guest
```

Output The following shows typical output.

Example output from show atmf links guest

node1#sh atmf links guest					
Guest Link Information:					
DC = Discovery configuration					
S = static D = dynamic					
Local Port	Guest Class	Model Type	DC	MAC Address	IP / IPv6 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

Parameters in the output from show atmf links guest

Parameter	Description
Local Port	The port on the parent node that connects to the guest.
Guest Class	The name of the ATMF guest-class that has been assigned to the guest node by the atmf guest-class command.
Model Type	The model type of the guest node, as entered by the modeltype command. Can be one of the following: • alliedware • aw+ • tq • other
DC	The discovery method as applied by the discovery command. This can be either dynamic (D) or static (S).
MAC Address	The MAC address of the guest node.
IP / IPv6 Address	The IP address of the guest node.

Related commands

- atmf guest-class**
- discovery**
- http-enable**
- username (atmf-guest)**
- modeltype**
- switchport atmf-guestlink**
- show atmf backup guest**

show atmf links guest detail

Overview This command displays detailed information about guest nodes visible to an AMF device.

Syntax `show atmf links guest detail [interface <interface-range>]`

Parameter	Description
<code>interface <interface-range></code>	Select a specific range of ports to display information about guest nodes.

Mode User Exec and Privileged Exec

Usage notes Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests detail](#).

Note that the parameters that are displayed depend on the guest node's model and state.

Example To display detailed information about AMF guests, use the command:
`node1# show atmf links guest detail`

Output The following shows typical output.

Example output from show atmf links guest detail

```
node1#show atmf links guest detail

Detailed Guest Link Information:

Interface                : port1.0.13
Link State               : Down
Class Name               : test
Model Type               : Other
Discovery Method         : Static
IP Address               : 192.168.1.13
Node State               : Down

Interface                : port1.0.5
Link State               : Full
Class Name               : tq_device
Model Type               : TQ
Discovery Method         : Dynamic
IP Address               : 192.168.1.221
Username                 : manager
Login Fallback           : Yes
Node State               : Full
Backup Supported         : Yes
MAC address              : 001a.ebab.d2e0
Device Type              : AT-TQ4600
Description               : AP221
Firmware Version         : 3.2.1 B02
HTTP port                : 80
```

Parameters in the output from show atmf links guest detail

Parameter	Description
Interface	The port on the parent node that connects to the guest.
Link State	The state of the link to the guest node; one of: • Down: The physical link is down. • Up: The physical link has come up, but it is still during a timeout period that is enforced to allow other links to come up. • Learn: The timeout period described above has elapsed, and the link is now learning information from the AMF guest node. You can see what information it is learning from the "Node State" field below. • Full: The node connected by this link has joined the AMF network. • Fail: The port is physically up but something has prevented the guest node from joining the AMF network.
Class Name	The name of the ATMF guest-class that has been assigned to the guest node by the atmf guest-class command.

Parameter	Description
Model Type	The model type of the guest node, as entered by the modeltype command. The mode type can be one of the following: - alliedware - aw+ - onvif - tq - other
Discovery Method	The discovery method as applied by the discovery command. This can be either dynamic or static.
IP Address	The IP address of the guest node.
Username	The user name configured on the guest node.
Login Fallback	Whether the guest node supports Login Fallback. For TQ model guest nodes, when login fallback is enabled, if a guest node is replaced, then AMF logs in to the new TQ using the factory default manager/friend settings. The new TQ is then discovered and managed as an AMF guest node by an AMF master or member. This means any backed up settings for the replaced guest node can also be recovered.
Node state	The state of the guest node; one of: - Down: The initial state when a link to a guest node is first configured. This is also the state if the physical link goes down. - Getting IP: The AMF device is in the process of retrieving the IP address of the guest node. - Getting Mac: The AMF device is in the process of retrieving the MAC address of the guest node. - Getting Info: The AMF device is in the process of retrieving any other available information from the guest (firmware version etc). The information available depends on what device the guest node is. - Full: The AMF device has retrieved all necessary information and the guest node has joined the AMF network. Once this state is reached, the Link State also changes to "Full". - Failure: The physical link is up but the AMF member has failed to retrieve enough information to allow the guest node to join the AMF network.
Backup Supported	Whether the guest node supports AMF backup functionality.
MAC Address	The MAC address of the guest node.
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

Parameter	Description
	shows what a user entered as the type of device they intended this guest node to be.
Description	By default, this is a concatenation of the guest node's parent node and the port to which it is attached. You can change it by configuring a description on the port.
Serial Number	The serial number of the guest node.
Firmware Name	The name of the firmware operating on the guest node.
Firmware Version	The version of the firmware operating on the guest node.
HTTP port	The HTTP port as specified with the http-enable command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).

Related commands

- [atmf guest-class](#)
- [discovery](#)
- [http-enable](#)
- [username \(atmf-guest\)](#)
- [modeltype](#)
- [switchport atmf-guestlink](#)
- [show atmf backup guest](#)

Command changes Version 5.5.0-1.1: **Login Fallback** parameter added

show atmf links statistics

Overview This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

Syntax show atmf links statistics [interface [*<port-number>*]]

Parameter	Description
interface	Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports) will be displayed.
<i><port-number></i>	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
```

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	
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 link	Receive	Receive Dropped	Transmit	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
```

Sample output from the show atmf links statistics command for interface port1.0.4

```
device1# show atmf links statistics interface port1.0.4
```

ATMF Port Statistics:

		Transmit	Receive
port1.0.4	Crosslink Hello	231	232
port1.0.4	Crosslink Hello Domain	116	116
port1.0.4	Crosslink Hello Uplink	116	115
port1.0.4	Hello Link	0	0
port1.0.4	Arealink Hello	0	0

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.
	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
```

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 Name      Device Type      ATMF Master  SC   Parent Domain      Node 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
```

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      SC      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
```

Sample output from show atmf nodes guest

```
node1#show atmf nodes guest

Guest Information:
Device      MAC      Parent      Port      IP/IPv6
Name        Address      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
```

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 The following shows typical output.

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 The following shows typical output.

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
```

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
```

Parameters in the output from show atmf secure-mode

Parameter	Description
Secure Mode Status	Shows the status of secure mode, Enabled or Disabled.
Certificate Expiry	Certificate expiry time. Set with atmf secure-mode certificate expiry
Certificates Total	Total number of certificates.
Certificates Revoked	Certificates that have been revoked by the AMF master.
Certificates Rejected	Certificates that have been rejected by the AMF master.
Certificates Active	Certificates that are currently active.
Provisional Authorization	Number of nodes with provisional authorization. For more information use the show atmf authorization provisional command.
Pending Requests	Number of nodes waiting for authorization on the AMF master. For more information use the show atmf authorization pending command.
Trusted Master	List of trusted masters in the AMF area.

Parameter	Description
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 The following shows typical output.

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.
```

Parameters in the output from show atmf secure-mode audit link

Parameter	Description
ATMF Secure Mode Audit	A list of security recommendations to secure the AMF network. Items prefaced with Warning need to be fixed. In the sample above the default username and password, and telnet, should be disabled.
ATMF Secure Mode Log Events	A list of recorded secure mode log events.

Related commands [show atmf secure-mode](#)

Command changes Version 5.4.7-0.3: command added

show atmf secure-mode audit link

Overview Use this command to detect security vulnerabilities by identifying devices that are connected to a secure mode node that are not in secure mode or are not authorized.

Syntax show atmf secure-mode audit link

Mode Privileged Exec

Example To display AMF secure mode link audits for a node, use the command
awplus# show atmf secure-mode audit link

Output The following shows typical output.

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

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 The following shows typical output.

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	Active
	master_2	4 Mar 2017	
area_1_node_2	master_1	11 Mar 2017	Revoked
	master_2	4 Mar 2017	
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

Parameters in the output from show atmf secure-mode certificates

Parameter	Description
Node Name	Name of AMF node the certificate was issued to.
Signer	Name of AMF master that issued the certificate.
Expires	Certificate expiry date.
Status	The status column will display Active before a member node is trusted, and can be accessed using AMF commands. Valid statuses are Active, Revoked, and Rejected.

Output The following shows typical output.

**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
```

**Parameters in the output from show atmf secure-mode
certificates detail**

Parameter	Description
MAC Address	MAC address of AMF node.
Status	The device status will show Active if a member node is trusted, and can be accessed using AMF commands. Valid statuses are Active, Revoked, and Rejected.
Serial Number	Device serial number.
Product	Device product type.
Key Fingerprint	AMF node key fingerprint.
Flags	Internal AMF information.
Signer	Name of AMF master that issued the certificate.
Expiry Date	Certificate expiry date.

Related commands

- [atmf authorize](#)
- [atmf secure-mode](#)
- [atmf secure-mode certificate expire](#)
- [atmf secure-mode certificate renew](#)
- [clear atmf secure-mode certificates](#)
- [show atmf secure-mode sa](#)

Command changes Version 5.4.7-0.3: command added

show atmf secure-mode sa

Overview Use this command to display the security associations on the network. This is the list of links and neighbors that are trusted.

Syntax `show atmf secure-mode sa [detail] [link|neighbor|broadcast]`

Parameter	Description
detail	Display detailed security association information.
link	Display security associations for type links.
neighbor	Display security associations for type neighbors.
broadcast	Display security associations for type broadcast.

Mode Privileged Exec

Example To display an overview of AMF secure mode security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa
```

To display a detailed overview of AMF secure mode neighbor security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa detail neighbor
```

Output The following shows typical output.

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

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

Parameters in the output from show atmf secure-mode sa

Parameter	Description
Type	Security Association (SA) types: • Link - SA for link • CrossLink - SA for crosslink • AreaLink - SA for area link • Neighbor Node - SA for node neighbor relationship • Neighbor Gateway - SA for gateway neighbor relationship • Neighbor Cntl-Master - SA for controller/master neighbor relationship • Broadcast - SA for working-set broadcast requests
State	Current state of the Security Association. The state must be Complete before a member node is trusted, and can be accessed using AMF commands. • CA Exchg Init - SA is ready to begin the SA exchange process • CA Exchg - SA is currently exchanging CAs • Cert Exchg - SA is currently exchanging certificates • Key Exchg - SA is currently exchanging ephemeral keys • Complete - SA exchange has completed
ID	Security Association ID. • For Neighbor types this is the remote node ID. • For Link types this is the local ifindex. • For Broadcast type this is always 4095.
Details	Human readable translation of ID. • For Neighbor types this is the node name • For Link types this is the interface name
Remote MAC Address	MAC address of the remote partner of the security association.
Flags	Internal AMF information.

Related commands [atmf secure-mode](#)
[show atmf secure-mode](#)
[show atmf secure-mode certificates](#)

Command changes Version 5.4.7-0.3: command added

show atmf secure-mode statistics

Overview Use this command to display AMF secure mode statistics. These statistics are from when AMF secure mode was first enabled or the statistics were cleared with the **clear atmf secure-mode statistics** command.

Syntax show atmf secure-mode statistics

Mode Privileged Exec

Example To display AMF secure mode statistics on a master or member node, use the command:

```
awplus# show atmf secure-mode statistics
```

Output The following shows typical output.

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 The following shows typical output.

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
```

Sample output from the show atmf tech command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : ATMF_NET
Node Name              : node1
Role                   : Master
Current ATMF Nodes    : 8

ATMF Technical information:

Network Name           : ATMF_NET
Domain                 : node1's domain
Node Depth             : 0
Domain Flags           : 0
Authentication Type    : 0
MAC Address            : 0014.2299.137d

Board ID               : 287
Domain State           : DomainController
Domain Controller      : node1
Backup Domain Controller : node2
Domain controller MAC   : 0014.2299.137d
Parent Domain          : -
Parent Domain Controller : -
Parent Domain Controller MAC : 0000.0000.0000
Number of Domain Events : 0
Crosslink Ports Blocking : 0
Uplink Ports Waiting on Sync : 0

Crosslink Sequence Number : 7
Domains Sequence Number   : 28
Uplink Sequence Number    : 2
Number of Crosslink Ports : 1
Number of Domain Nodes    : 2
Number of Neighbors       : 5
Number of Non Broadcast Neighbors : 3
Number of Link State Entries : 1
Number of Up Uplinks      : 0
Number of Up Uplinks on This Node : 0
DBE Checksum              : 84fc6
Number of DBE Entries     : 0
...
```

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.

Parameter	Definition
Role	The role configured on the device within the AMF - either master or member.
Current ATMF Nodes	A count of the AMF nodes in the AMF network.
Node Address	The identity of a node (in the format name.atmf) that enables its access it from a remote location.
Node ID	A unique identifier assigned to an AMF node.
Node Depth	The number of nodes in the path from this node to the core domain.
Domain State	A node's state within an AMF Domain - either controller or backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between nodes of different domains (up/down links). VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. Management Subnet - the Network prefix for the subnet. Management IP Address - the IP address allocated for this traffic. Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. Domain Subnet - the Subnet address used for this traffic. Domain IP Address - the IP address allocated for this traffic. Domain Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)
Device Type	Shows the Product Series Name.
ATMF Master	Indicates the node's membership of the core domain (membership is indicated by Y)
SC	Shows switch configuration: • C - Chassis (such as SBx8100 series) • S - Stackable (VCS)

Parameter	Definition
	• N - Standalone
Parent	A node that is connected to the present node's uplink, i.e. one layer higher in the hierarchy.
Node Depth	Shows the number of nodes in path from the current node to the Core domain.

NOTE: The command can produce very large output. For this reason only the most significant terms are defined in this table.

show atmf virtual-links

Overview This command displays a summary of all virtual links (L2TP tunnels) currently in the running configuration.

Syntax show atmf virtual-links [macaddr]
show atmf virtual-links [id <1-4094>] [remote-id <1-4094>]
show atmf virtual-links detail [id <1-4094>]

Parameter	Description
macaddr	Display the virtual AMF links' MAC addresses.
id <1-4094>	ID of the local virtual link.
remote-id <1-4094>	ID of the remote virtual link
detail	Display information about a specific virtual link ID or range of virtual link IDs. Displays information such as: local and remote IP address, link type, packets received and transmitted.

Mode Privileged Exec

Example 1 To display AMF virtual links, use the command:

```
node_1# show atmf virtual-links
```

Example output from show atmf virtual-links

ATMF Virtual-Link Information:						
Local Port	Local ID	Local IP	Remote ID	Remote IP	Tunnel Protect	Tunnel State
vlink1	1	172.16.24.2	2	1.0.0.2	-	Complete
vlink2	2	172.16.24.2*	10	172.16.24.3*	ipsec	Complete
vlink3	3	(eth0)*	1	1.2.3.4	-	AcquireLocal
* = Dynamic Address.						
Virtual Links Configured: 3						

In the above example, a centrally located switch has the IP address space 192.0.2.x/24. It has two VLANs assigned the subnets 192.0.2.33 and 192.0.2.65 using the prefix /27. Each subnet connects to a virtual link. The first link has the IP address 192.168.1.1 and has a Local ID of 1. The second has the IP address 192.168.2.1 and has the Local ID of 2.

Example 2 To display details about AMF virtual link with ID 1, use the command:

```
node_1# show atmf virtual-links detail id 1
```

Example output from show atmf virtual-links

Virtual Link Detailed Information:			
ID 1	Description	:	None
ID 1	Local IP Address	:	192.168.5.1
ID 1	Remote ID	:	1
ID 1	Remote IP Address	:	192.168.5.20
ID 1	Link Type	:	virtual-link
ID 1	Packets Received	:	236465
ID 1	Packets Transmitted	:	192626

Example 3 To display AMF virtual links' MAC address information, use the command:

```
node_1# show atmf virtual-links macaddr
```

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

Parameters in the output from show atmf virtual-links

Parameter	Definition
Local Port	The tunnel name e.g. vlink1, vlink2, equivalent to an L2TP tunnel.
Local ID	The local ID of the virtual link. This matches the vlink<number>
Tunnel Protect	Tunnel protection protocol.
Tunnel State	The operational state of the vlink (either Up or Down). This state is always displayed once a vlink has been created.
mac addr	AMF virtual links terminate on an internal soft bridge. The "show atmf virtual-links macaddress" command displays MAC Address information.
is local?	Indicates whether the MAC displayed is for a local or a remote device.
ageing timer	Indicates the current aging state for each MAC address.

Related commands [atmf virtual-link](#)

show atmf working-set

Overview This command displays the nodes that form the current AMF working-set.

Syntax show atmf working-set

Mode Privileged Exec

Example To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

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
```

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
```

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 **show atmf links guest**
commands

switchport atmf-arealink

Overview This command enables you to configure a port or aggregator to be an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network.

Use the **no** variant of this command to remove any AMF area link that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

Syntax switchport atmf-arealink remote-area <area-name> vlan <2-4094>
no switchport atmf-arealink

Parameter	Description
<area-name>	The name of the remote area that the port is connecting to.
<2-4094>	The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link.

Default No arealinks are configured.

Mode Interface Configuration for a switchport, a static aggregator, or a dynamic channel group.

Usage notes Run this command on the port or aggregator at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

NOTE: See the command to configure an AMF area link on an AR-series Eth interface.

Example To make switchport port1.0.2 an arealink to the 'Auckland' area on VLAN 6, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.2
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

To remove switchport port1.0.1 as an AMF area link, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.1
controller-1(config-if)# no switchport atmf-arealink
```

Related commands

- atmf area**
- atmf area password**
- atmf virtual-link**
- show atmf links**

switchport atmf-crosslink

Overview This command configures the selected port, statically aggregated link or dynamic channel group (LACP) to be an AMF crosslink. Running this command will automatically place the port or aggregator into trunk mode (i.e. **switchport mode trunk**).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

Syntax switchport atmf-crosslink
no switchport atmf-crosslink

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage notes Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the **switchport trunk native vlan none** 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 (atmf-guest)**
- modeltype**
- show atmf links guest**
- show atmf guests**

switchport atmf-link

Overview This command enables you to configure a port or aggregator to be an up/down AMF link. Running this command will automatically place the port or aggregator into trunk mode. If the port was previously configured in access mode, the configured access VLAN will be removed.

Use the **no** variant of this command to remove any AMF link that may exist for the selected port or aggregated link.

Syntax switchport atmf-link
no switchport atmf-link

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage notes Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

Within each domain, cross-links between AMF nodes define those nodes as siblings within the same domain. You can form rings by combining cross-links with up/down links and/or virtual links, as long as each AMF domain links upwards to only a single parent domain. Each domain may link downwards to multiple child domains.

NOTE: See the command to configure an AMF up/down link on an AR-series Eth interface.

Example To configure switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```

To remove switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# no switchport atmf-link
```

Related commands [atmf-link](#)
[show atmf detail](#)
[show atmf links](#)

type atmf guest

Overview This command configures a trigger to activate when an AMF guest node joins or leaves.

Syntax type atmf guest {join|leave}

Parameter	Description
join	AMF guest node joins.
leave	AMF guest node leaves.

Mode Trigger Configuration

Example To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

Related commands [show trigger](#)

Command changes Version 5.5.1-1.1: command added

type atmf node

Overview This command configures a trigger to activate when an AMF node joins or leaves.

Syntax type atmf node {join|leave}

Parameter	Description
join	AMF node joins.
leave	AMF node leaves.

Mode Trigger Configuration

Example 1 To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
```

```
AMF-Net[3](config)# trigger 5
```

```
AMF-Net[3](config-trigger)# type atmf node leave
```

```
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
```

```
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
```

```
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=====
node1:
=====

TR# Type & Details      Description      Ac Te Tr Repeat      #Scr Days/Date
-----
001 Periodic (2 min)    Periodic Status Chk Y  N  Y Continuous    1  smtwtfS
005 ATMF node (leave)  E-mail on ATMF Exit Y  N  Y Continuous    1  smtwtfS
-----

=====
Node2, Node3,
=====

TR# Type & Details      Description      Ac Te Tr Repeat      #Scr Days/Date
-----
005 ATMF node (leave)  E-mail on ATMF Exit Y  N  Y Continuous    1  smtwtfS
-----
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
=====
Node1:
```

```
=====

trigger 1
  type periodic 2
  script 1 atmf.scp
trigger 5
  type atmf node leave
description "E-mail on ATMF Exit"
  script 1 email_me.scp
!

=====
Node2, Node3:
=====

trigger 5
  type atmf node leave
description "E-mail on ATMF Exit"
  script 1 email_me.scp
!
```

Related [show trigger](#)
commands

undebbug atmf

Overview This command is an alias for the **no** variant of the **debug atmf**.

username (atmf-guest)

Overview This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. The password must be between 1 and 32 characters and will allow spaces.

Syntax username <name> password [8] <userpass>
no username

Parameter	Description
<name>	User name of the guest node.
8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form.
<userpass>	The password to be entered for the guest node.

Default No usernames are configured

Mode AMF Guest Configuration

Example To assign the user name 'reception' and the password of 'secret' to an AMF guest node that has the guest class of 'phone1' use the following commands:

```
node1# configure terminal
node1(config)# amf guest-class phone1
node1(config-atmf-guest)# username reception password secret
```

To remove a guest node username and password for the user guest class 'phone1', use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class phone1
node1(config-atmf-guest)# no username
```

Related commands

- [show atmf links detail](#)
- [atmf guest-class](#)
- [switchport atmf-guestlink](#)
- [show atmf links guest](#)
- [show atmf nodes](#)

30

STOAT Commands

- Contents**
- **Introduction** on page 1583
 - **clear stoat collector session counters** on page 1584
 - **description (stoat-dest)** on page 1585
 - **key (stoat-dest)** on page 1586
 - **name-check (stoat-dest)** on page 1587
 - **service stoat** on page 1588
 - **show stoat collector** on page 1589
 - **show stoat destinations** on page 1592
 - **shutdown (stoat-dest)** on page 1594
 - **stoat collector enable** on page 1595
 - **stoat collector expiry-period** on page 1596
 - **stoat collector key** on page 1597
 - **stoat collector trustpoint** on page 1599
 - **stoat destination** on page 1600
 - **stoat discovery** on page 1602
 - **trustpoint (stoat-dest)** on page 1603
 - **unique-id** on page 1604

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Device Discovery using STOAT (Standardized Topology Organizer and Transport).

Using LLDP and DHCP Snooping, STOAT can discover and gather information about devices in the local network. These devices may include IP cameras, IP phones, PCs, laptops, Wi-fi access points, printers, and so on.

Vista Manager EX merges the data from STOAT and existing discovery methods such as AMF, and AMF Plus Device Discovery, to provide a single, accurate and more complete view of the network.

For more information, see the [Device Discovery using STOAT Feature Overview and Configuration Guide](#).

clear stoat collector session counters

Overview Use this command to clear the STOAT transport session counters.

Syntax clear stoat collector session counters [<1-4294967295>]

Parameter	Description
<1-4294967295>	Session ID

Mode Privileged Exec

Example To clear all STOAT transport session counters, use the command:

```
awplus# clear stoat collector session counters
```

To clear a specific STOAT transport session counter, use the command:

```
awplus# clear stoat collector session counters 234234234
```

Related commands

- [stoat collector trustpoint](#)
- [show stoat collector](#)
- [stoat collector expiry-period](#)
- [stoat collector key](#)

Command changes Version 5.5.3-1.1: command added

description (stoat-dest)

Overview Use this command to add an informative description to a STOAT destination.

Use the **no** variant of this command to remove a description from a STOAT destination.

Syntax `description <description>`
`no description`

Parameter	Description
<code><description></code>	A word or phrase that uniquely identifies this STOAT destination or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters.

Default Not set.

Mode STOAT Destination Configuration

Example To add the description 'chc-collector-1' to a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# description chc-collector-1
```

To remove the description from a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no description
```

Related commands [stoat destination](#)

Command changes Version 5.5.3-1.1: command added

key (stoat-dest)

Overview Use this command to configure a key to use with a STOAT destination. The key allows the STOAT collector to authenticate this device as a valid source. The destination will not attempt to connect if no key is set.

A matching key must be configured on the STOAT collector device.

Use the **no** variant of this command to remove a key for a STOAT destination.

Syntax key [8] <key-string>
no key

Parameter	Description
8	Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 8 to 80 characters.

Default Not set.

Mode STOAT Destination Configuration

Example To configure the key 'verysecret' for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# key verysecret
```

To remove the key for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no key
```

Related commands [stoat collector key](#)
[stoat destination](#)

Command changes Version 5.5.3-1.1: command added

name-check (stoat-dest)

Overview Use this command to enable or disable certificate name checking for the server certificate received from the STOAT collector.

Use the **no** variant of this command to disable name checking for the server certificate received from the STOAT collector.

Syntax name-check
no name-check

Default Disabled.

Mode STOAT Destination Configuration

Usage notes If enabled, the received server certificate must contain the address configured for this STOAT destination . This setting only takes effect if the STOAT destination has been configured with a trustpoint.

Example To enable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# name-check
```

To disable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# no name-check
```

Related commands [service stoat](#)

Command changes Version 5.5.3-1.1: command added

service stoat

Overview Use this command to enable or disable Standardized Topology Organizer and Transport (STOAT) functionality on a device. Once enabled, the device will accept STOAT collector and STOAT source configuration.

Use the **no** variant of this command to disable STOAT functionality on a device.

Syntax service stoat
no service stoat

Default Disabled.

Mode Global Configuration

Example To enable STOAT functionality on a device, use the commands:

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

To disable STOAT functionality on a device, use the commands:

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

Related commands [stoat collector trustpoint](#)
[stoat collector expiry-period](#)
[stoat collector key](#)
[show stoat collector](#)

Command changes Version 5.5.3-1.1: command added

show stoat collector

Overview Use this command to see the operational status of the STOAT collector.

Syntax show stoat collector [sessions|keys]

Parameter	Description
sessions	Active session information
keys	Authentication key information

Mode Privileged Exec

Example To show the STOAT collector status information, use the command:

```
awplus# show stoat collector
```

To show the STOAT collector active session information, use the command:

```
awplus# show stoat collector sessions
```

To show the STOAT collector authentication key information, use the command:

```
awplus# show stoat collector keys
```

Output **Example output from show stoat collector**

```
awplus#show stoat collector
STOAT Collector Information:
-----
Status      : Enabled
Expiry-period : 60 seconds
Trustpoint   : default-selfsigned
```

Example output from show stoat collector sessions

```
awplus#show stoat collector sessions
STOAT Collector Session Information:
-----
Sessions created           : 2
Sessions expired           : 0
Sessions failed            : 0
Sessions failed sync authentication : 0
Sessions failed update     : 0
Sessions failed update authentication : 0

Session ID                 : 3F4B5C27
Source Name                : alice
State                     : Active
Counters
  Update success           : 0
  Update authentication failure : 0
  Update failure           : 0
  RX payload bytes         : 11
  RX payload apteryx set failure : 0
  RX payload json parse failure : 0
  RX payload json decode failure : 0

Session ID                 : 23DFBD7B
Source Name                : bob
State                     : Active
Counters
  Update success           : 0
  Update authentication failure : 0
  Update failure           : 0
  RX payload bytes         : 0
  RX payload apteryx set failure : 0
  RX payload json parse failure : 0
  RX payload json decode failure : 1
```

Example output from show stoat collector keys

```
awplus#show stoat collector keys
STOAT Collector Key Information:
-----
Key                                Description                                Last Used Time
                                   (H:M:S ago)
-----
CoA4E6riSbdWzzetHhHM5F5WdBFPXX2DH6jNzZmYtns= "generated key"                00:12:52
secret-key                                "super secret key"              -
```

Related commands **service stoat**
 stoat collector expiry-period
 stoat collector enable

Command changes Version 5.5.3-1.1: command added

show stoat destinations

Overview Use this command to see the operational status of the configured STOAT destinations.

Syntax show stoat destinations [detail]

Parameter	Description
detail	Show detailed information

Mode Privileged Exec

Example To show summary information about STOAT destinations, use the command:

```
awplus# show stoat destinations
```

To show detailed information about STOAT destinations, use the command:

```
awplus# show stoat destinations detail
```

Output The following shows typical output.

Example output from show stoat destinations

```
awplus#show stoat destinations
STOAT Destination Summary Information:
-----|
Address      : 192.168.0.12
State        : Hold

Address      : 192.168.0.2
State        : Active
```

Example output from show stoat destinations detail

```
awplus#show stoat destinations detail
STOAT Destination Summary Information:
-----|
Address      : 192.168.0.12
State        : Hold
Session ID   : 0
Expiry-period : 0 seconds
Counters:
  Sync OK           : 0
  Sync failed - unreachable : 6612
  Sync failed - authentication : 0
  Sync failed - bad response  : 0
  Update OK         : 0
  Update failed - unreachable : 0
  Update failed - authentication : 0
  Update failed - unknown session : 0
  RX bytes          : 0
  TX bytes          : 0
Address      : 192.168.0.2
State        : Active
Session ID   : 200558F4
Expiry-period : 60 seconds
Counters:
  Sync OK           : 139
  Sync failed - unreachable : 10
  Sync failed - authentication : 0
  Sync failed - bad response  : 0
  Update OK         : 32773
  Update failed - unreachable : 52
  Update failed - authentication : 0
  Update failed - unknown session : 81
  RX bytes          : 4099
  TX bytes          : 16787801
```

Related commands [stoat destination shutdown \(stoat-dest\)](#)

Command changes Version 5.5.3-1.1: command added

shutdown (stoat-dest)

Overview Use this command to disable a STOAT destination.
Use the **no** variant of this command to enable a STOAT destination.

Syntax shutdown
no shutdown

Default Enabled (no shutdown)

Mode STOAT Destination Configuration

Example To enable the STOAT destination 192.0.2.6, use the commands:
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no shutdown

Related commands [stoat destination](#)
[show stoat destinations](#)

Command changes Version 5.5.3-1.1: command added

stoat collector enable

Overview Use this command to start or stop the Standardized Topology Organizer and Transport (STOAT) collector functionality on a device.

Note: The device must be able to receive requests from STOAT sources before this command is used. To enable a device to receive requests from STOAT, use the [service stoat](#) command.

Use the **no** variant of this command to stop the STOAT collector functionality on a device.

Syntax stoat collector enable
no stoat collector enable

Default Disabled.

Mode Global Configuration

Usage notes The STOAT feature is responsible for discovering devices and network topology, organizing that information into a standardized format, and transporting it to a central location for use. AMF uses STOAT data to allow non-AMF devices and their links to be displayed in the AMF topology map.

There are two types of STOAT device:

- **Collector** - receives and aggregates topology data
- **Source** - sends data to a collector. The data contains information that it knows about itself and has learned through discovery protocols

Example To start the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector enable
```

To stop the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector enable
```

Related commands [stoat collector trustpoint](#)
[show stoat collector](#)
[stoat collector expiry-period](#)
[stoat collector key](#)

Command changes Version 5.5.3-1.1: command added.

stoat collector expiry-period

Overview Use this command to modify the session expiry-period for all of the STOAT collector's sessions.

Use the **no** variant of this command to revert to the default expiry-period of 60 seconds.

Syntax stoat collector expiry-period <10-300>
no stoat collector expiry-period

Parameter	Description
<10-300>	Expiry-period in seconds (default: 60)

Default 60 seconds.

Mode Global Configuration

Example To configure an expiry-period of 15 seconds, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# stoat collector expiry-period 15
```

To revert the expiry-period to its default of 60 seconds, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no stoat collector expiry-period
```

Related commands

- [service stoat](#)
- [stoat collector trustpoint](#)
- [stoat collector key](#)
- [stoat collector enable](#)
- [show stoat collector](#)

Command changes Version 5.5.3-1.1: command added

stoat collector key

Overview Use this command to configure the authentication key used by the STOAT collector.

Use the **no** variant of this command to remove a STOAT authentication key.

Syntax stoat collector key [8]{auth-key|generate} [description <description>]
no stoat collector key [8]{auth-key|generate} [description <description>]

Parameter	Description
8	Specifies a key in encrypted format instead of plain text.
auth-key	Authentication key
generate	Let STOAT generate a key
description	Add a useful description
<description>	The useful description text

Default Not set.

Mode Global Configuration

Example To configure a plain-text key 'secret-key' with no description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key
```

To configure a plain-text key 'secret-key' with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key description 'this
is my secret key'
```

To **generate** a key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key generate description 'my
generated key'
```

To configure an encrypted key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZ0J-eJ00JslX0N3E= description 'my
encrypted key'
```

To remove a configured encrypted key, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZ0J-eJ00JslX0N3E=
```

Output The following shows typical output.

Example output from stoat collector key generate

```
awplus(config)# stoat collector key generate
NttWCIS0KsyQ1-1_98qi4HcVdMRykeaE8IKfPe1Xv9o
```

Related commands

- [service stoat](#)
- [stoat collector trustpoint](#)
- [stoat collector expiry-period](#)
- [stoat collector enable](#)
- [show stoat collector](#)

Command changes Version 5.5.3-1.1: command added

stoat collector trustpoint

Overview Use this command to add a crypto PKI trustpoint containing a server certificate and a key to the STOAT collector. This enables secure HTTPS API communication between the STOAT collector and STOAT source.

Use the **no** variant of this command to remove a configured PKI trustpoint from a STOAT collector.

Syntax stoat collector trustpoint <trustpoint-name>
no stoat collector trustpoint

Parameter	Description
<trustpoint-name>	PKI trustpoint name.

Mode Global Configuration

Example To add an existing PKI trustpoint called 'chc' to the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector trustpoint chc
```

To remove a configured PKI trustpoint from the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector trustpoint
```

Related commands [crypto pki authenticate](#)
[crypto pki enroll](#)
[crypto pki trustpoint](#)

Command changes Version 5.5.3-1.1: command added

stoat destination

Overview Use this command to configure a remote STOAT collector destination.

Use the **no** variant of this command to remove a STOAT collector destination.

When VRF-lite is configured, you can apply this command to a specific VRF instance.

Syntax `stoat destination {<ip-address>|<host-name>|<ipv6-address>} [vrf <vrf-name>]`
`no stoat destination {<ip-address>|<host-name>|<ipv6-address>} [vrf <vrf-name>]`

Parameter	Description
<code><ip-address></code>	The IPv4 address, using the format A.B.C.D.
<code><host-name></code>	The host name specified in FQDN (Fully Qualified Domain Name). For example, manager.your.domain.com.
<code><ipv6-address></code>	The IPv6 address, using the format X:X::X:X.
<code>vrf</code>	Specify a VRF instance.
<code><vrf-name></code>	The name of the specific VRF instance.

Default Not set.

Mode Global Configuration

Example To configure a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 10.0.0.1
```

To remove a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 10.0.0.1
```

To configure a remote STOAT collector at IP address 10.0.0.1 on VRF red, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 10.0.0.1 vrf red
```

To configure a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination stoat.com
```

To remove a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination stoat.com
```

To configure a remote STOAT collector at 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 2001:db8::1
```

To remove a remote STOAT collector at 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 2001:db8::1
```

Related commands [stoat collector key](#)
[show stoat collector](#)
[stoat discovery](#)

Command changes Version 5.5.3-1.1: command added

stoat discovery

Overview Use this command to enable a device to import Standardized Topology Organizer and Transport (STOAT) discovery information learned by a given protocol. This command allows the device to act as a STOAT collector. STOAT collectors receive and aggregate topology data used in the AMF topology map.

Use the **no** variant of this command to disable the import of STOAT discovery information learned by a given protocol.

Syntax `stoat discovery lldp`
`stoat discovery wireless`
`no stoat discovery lldp`
`no stoat discovery wireless`

Parameter	Description
lldp	Import information learned through the LLDP protocol.
wireless	Import information learned by Wireless Manager

Default Disabled.

Mode Global Configuration

Example To enable a device to import information learned by the LLDP protocol, use the commands:

```
awplus# configure terminal
awplus(config)# stoat discovery lldp
```

To disable a device from importing information learned by the LLDP protocol, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat discovery lldp
```

Related commands [lldp run](#)
[stoat destination](#)

Command changes Version 5.5.3-1.1: command added
Version 5.5.3-2.1: **dot1x** and **wireless** parameters added

trustpoint (stoat-dest)

Overview Use this command to specify the trustpoint to use when authenticating the STOAT collector. If no trustpoint is specified, the STOAT collector will be implicitly trusted without authentication.

Use the **no** variant of this command to stop the use of trustpoints with a specified STOAT destination.

Syntax trustpoint <trustpoint-name>
no trustpoint

Parameter	Description
<trustpoint-name>	Name of the trustpoint.

Default Not set.

Mode STOAT Destination Configuration

Example To configure the STOAT destination 192.0.2.6 to use trustpoint 'chc', use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# trustpoint chc
```

To stop the use of trustpoints with STOAT destination 192.0.2.6 use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no trustpoint
```

Related commands [stoat collector trustpoint](#)
[stoat destination](#)
[name-check \(stoat-dest\)](#)

Command changes Version 5.5.3-1.1: command added

unique-id

Overview Use this command to generate a new unique ID for a device. This ID is used to uniquely identify a device in the STOAT topology.

Some circumstances may require you to generate a new unique ID, for example after recovering a device from an AMF provisioned backup.

Syntax unique-id

Mode Privileged Exec

Example To generate a new unique ID for a STOAT device, use the command:

```
awplus# unique-id
```

Related commands [service stoat](#)

Command changes Version 5.5.3-1.1: command added

31

Dynamic Host Configuration Protocol (DHCP) Commands

- Contents**
- **Introduction** on page 1607
 - **bootfile** on page 1608
 - **clear ip dhcp binding** on page 1609
 - **default-router** on page 1611
 - **dns-server** on page 1612
 - **domain-name** on page 1614
 - **host (DHCP)** on page 1615
 - **ip address dhcp** on page 1616
 - **ip dhcp bootp ignore** on page 1618
 - **ip dhcp globally-authoritative** on page 1619
 - **ip dhcp leasequery enable** on page 1620
 - **ip dhcp option** on page 1621
 - **ip dhcp pool** on page 1624
 - **ip dhcp-client default-route distance** on page 1625
 - **ip dhcp-client request vendor-identifying-specific** on page 1627
 - **ip dhcp-client vendor-identifying-class** on page 1628
 - **ip dhcp-relay agent-option** on page 1629
 - **ip dhcp-relay agent-option checking** on page 1631
 - **ip dhcp-relay agent-option remote-id** on page 1632
 - **ip dhcp-relay information policy** on page 1634
 - **ip dhcp-relay maxhops** on page 1636
 - **ip dhcp-relay max-message-length** on page 1637
 - **ip dhcp-relay server-address** on page 1639
 - **ip dhcp-relay short-lease** on page 1641
 - **ip dhcp-relay use-client-side-address** on page 1642
 - **ip dhcp-relay use-dhcp-relay-ip** on page 1644
 - **lease** on page 1645
 - **network (DHCP)** on page 1647
 - **next-server** on page 1648
 - **option** on page 1649
 - **probe enable** on page 1651
 - **probe packets** on page 1652
 - **probe timeout** on page 1653
 - **probe type** on page 1654
 - **range** on page 1655
 - **route** on page 1656

- **service dhcp-relay** on page 1657
- **service dhcp-server** on page 1658
- **short-lease-threshold** on page 1659
- **show counter dhcp-client** on page 1661
- **show counter dhcp-relay** on page 1663
- **show counter dhcp-server** on page 1668
- **show dhcp lease** on page 1671
- **show ip dhcp binding** on page 1672
- **show ip dhcp pool** on page 1674
- **show ip dhcp-relay** on page 1677
- **show ip dhcp server statistics** on page 1679
- **show ip dhcp server summary** on page 1682
- **subnet-mask** on page 1683
- **vrf** on page 1684

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**.

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

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>}`

Syntax (VRF-lite) `clear ip dhcp binding [vrf <name>|global] {ip <ip-address>|mac <mac-address>|all|pool <pool-name>|range <low-ip-address> <high-ip-address>}`

Parameter	Description
vrf	Display the output for a VRF instance
<name>	The name of the specific VRF instance.
global	Display the output for the Global VRF instance
ip <ip-address>	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.
mac <mac-address>	MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.
all	All DHCP bindings.
pool <pool-name>	Description used to identify DHCP server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks".
range <low-ip-address> <high-ip-address>	IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end of the range.

Mode User Exec and Privileged Exec

Usage A specific binding may be deleted by **ip** address or **mac** address, or several bindings may be deleted at once using **all**, **pool** or **range**.

Note that if you specify to clear the **ip** or **mac** address of what is actually a static DHCP binding, an error message is displayed. If **all**, **pool** or **range** are specified and one or more static DHCP bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

Examples To clear the specific IP address binding 192.168.1.1, use the command:

```
awplus# clear ip dhcp binding ip 192.168.1.1
```

To clear all dynamic DHCP entries, use the command:

```
awplus# clear ip dhcp binding all
```

Example (VRF-lite) To clear all dynamic binding from VRF red instance, use the command:

```
awplus# clear ip dhcp binding vrf red all
```

Related commands [show ip dhcp binding](#)

default-router

Overview This command adds a default router to the DHCP address pool you are configuring. You can use this command multiple times to create a list of default routers on the client's subnet. This sets the router details using the pre-defined option 3. Note that if you add a user-defined option 3 using the **option** command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified default router, or all default routers from the DHCP pool.

Syntax default-router <ip-address>
no default-router [<ip-address>]

Parameter	Description
<ip-address>	IPv4 address of the default router, in dotted decimal notation.

Mode DHCP Configuration

Examples To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```

dns-server

Overview This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6.

Note that if you add a user-defined option 6 using the **option**, 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><ip-address></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**, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

Syntax domain-name <domain-name>
no domain-name

Parameter	Description
<domain-name>	The domain name you wish to assign the DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode DHCP Configuration

Examples To add the domain name Nerv_Office to DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# domain-name Nerv_Office
```

To remove the domain name Nerv_Office from DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no domain-name Nerv_Office
```

Related commands

- default-router**
- dns-server**
- option**
- service dhcp-server**
- show ip dhcp pool**
- subnet-mask**

host (DHCP)

Overview This command adds a static host address to the DHCP address pool you are configuring. The client with the matching MAC address is permanently assigned this IP address. No other clients can request it.

The **no** variant of this command removes the specified host address from the DHCP pool. Use the **no host all** command to remove all static host addresses from the DHCP pool.

Syntax `host <ip-address> <mac-address>`
`no host <ip-address>`
`no host all`

Parameter	Description
<code><ip-address></code>	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D
<code><mac-address></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> <code><interface></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. Default: no default
<code>hostname</code> <code><hostname></code>	The hostname for the DHCP client on this interface. Typically this name is provided by the ISP. Default: no default

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To set the interface eth1 to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address dhcp
```

To stop the interface eth1 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 globally-authoritative

Overview Use this command to make the DHCP server globally authoritative. When the DHCP server is globally authoritative, it responds to all DHCP requests and inform messages, even if it has no DHCP pool for the request's subnet. If the server doesn't have an applicable DHCP pool, it can't assign an IP address, so it immediately responds with a NACK message.

Use the **no** variant of this command to stop the server from being globally authoritative. If you do that, the server will not respond to the above messages. This means the client will need to time out if it has sent one of the above messages, as it will not receive a reply.

Note that the server will:

- always be authoritative for DHCP requests and inform messages if it has a DHCP pool for the relevant subnet
- never be globally authoritative if the server is also configured as a relay agent, even if this command is enabled. In that case, it will only reply if the server has a DHCP pool for the relevant subnet. Otherwise, the server could respond to a message that was intended for the other server at the end of the relay agent.

Syntax ip dhcp globally-authoritative
no ip dhcp globally-authoritative

Default Enabled

Mode Global Configuration

Example To stop the server from being globally authoritative, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp globally-authoritative
```

Related commands [show ip dhcp server summary](#)

Command changes Version 5.5.5-1.1: command added

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”. Default: no default										
<option-type>	The option value. You must specify a value that is appropriate to the option type: <table><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: true, on, or enabled will set the flag. false, off or disabled will unset the flag.</td></tr></table>	ascii	An ASCII text string	hex	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.	ip	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.	integer	A number from 0 to 4294967295.	flag	A value that either sets (to 1) or unsets (to 0) a flag: true, on, or enabled will set the flag. false, off or disabled will unset the flag.
ascii	An ASCII text string										
hex	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.										
ip	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.										
integer	A number from 0 to 4294967295.										
flag	A value that either sets (to 1) or unsets (to 0) a flag: true, on, or enabled will set the flag. false, off or disabled will unset the flag.										

Mode Global Configuration

Examples To define a user-defined ASCII string option as option 66, without a name, use the command:

```
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><pool-name></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 for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes DHCP client interfaces can automatically add a default route with an AD of 1 into the IP Routing Information Base (RIB).

Any pre-existing default route(s) via alternative interfaces (configured with a higher AD) will no longer be selected as the preferred forwarding path for traffic when the DHCP based default route is added to the IP routing table.

This can be problematic if the DHCP client is operating via an interface that is only intended to be used for back-up interface redundancy purposes, such as an interface with lower bandwidth or a particular role like the management interface.

Use this command to set the AD of the default route (via a specific DHCP client interface) to a non-default (higher cost) value, ensuring any pre-existing default route(s) via any other interface(s) continue to be selected as the preferred forwarding path for network traffic.

When the command is used, the static default route is deleted from the RIB, the distance value of the route is modified to the configured distance value, then it is reinstalled into the RIB.

Examples To 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 for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes The DHCP client must be activated on the interface, using the **ip address dhcp** command, so that DHCP discovery packets are sent.

Example To add the vendor-identifying-specific request on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-client request vendor-identifying-specific
```

To remove the vendor-identifying-specific request on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-client request vendor-identifying-specific
```

Related commands **ip address dhcp**
ip dhcp-client vendor-identifying-class

Command changes Version 5.4.7-2.1: command added

ip dhcp-client vendor-identifying-class

Overview Use this command to add a vendor-identifying vendor class (option 124) to the DHCP discovery packets sent by an interface. This option places the Allied Telesis Enterprise number (207) into the discovery packet. Option 124, along with option 125, can be used to send vendor-specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-class from an interface.

Syntax ip dhcp-client vendor-identifying-class
no ip dhcp-client vendor-identifying-class

Default The vendor-identifying-class is not configured by default.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes The DHCP client must be activated on the interface, using the **ip address dhcp** command, so that DHCP discovery packets are sent.

Example To remove the vendor-identifying-class on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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: *ip dhcp-relay agent-optionip dhcp-relay information policy*

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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 relay agent listening on eth1 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To make the relay agent listening on eth1 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related commands **ip dhcp-relay agent-option**
ip dhcp-relay agent-option remote-id
ip dhcp-relay information policy
service dhcp-relay

ip dhcp-relay agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

Syntax ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_), and hash (#). Spaces are not allowed.

Default The Remote ID is set to the device's MAC address by default.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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: *ip dhcp-relay agent-optionip dhcp-relay information policy*

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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To make the DHCP Relay Agent listening on eth1 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Example To set the maximum number of hops to 5 for packets received on interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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: [ip dhcp-relay agent-option](#)

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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
<code><ipv4-address></code>	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.
<code><ipv6-address></code>	Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.
<code><server-interface></code>	Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 eth1 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

DHCP for IPv4

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

Examples: To enable the DHCP Relay Agent on your device to relay DHCP packets on interface eth1.2 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4, use the commands:

DHCPv6

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1.2
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4 from the list of servers available to the DHCP Relay Agent on interface eth1.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

Example: To disable DHCP relay on eth1, use the commands:

disabling DHCP relay

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay
```

Related commands [service dhcp-relay](#)

ip dhcp-relay short-lease

Overview Use this command to reduce the amount of time an IP address is assigned to a client device.

Long lease times can cause issues in dynamic networks where client devices frequently move between segments, such as VLANs. These device may retain an outdated IP address from its previous VLAN, disrupting communication.

This command is particularly useful in networks with a high turnover of devices or in environments where IP addresses are scarce.

Use the **no** variant of this command to remove the short lease time configuration.

Syntax `ip dhcp-relay short-lease <20-3600>`
`no ip dhcp-relay short-lease`

Parameter	Description
<20-3600>	The lease time for DHCP relay in seconds.

Default Not set

Mode Interface Configuration

Example To configure a DHCP Relay on interface vlan1 with a lease time of 200 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease 200
```

Related commands [show ip dhcp-relay](#)

Command changes Version 5.5.4-2.1: command added

ip dhcp-relay use-client-side-address

Overview Use this command to configure DHCP-Relay to use the client-side interface (that is the interface receiving the DHCP client packets) IP address as the source address of the relayed DHCP packets.

Use the **no** variant of this command to disable the use of the client-side interface IP address as the source IP address for relayed DHCP packets.

Syntax ip dhcp-relay use-client-side-address
no ip dhcp-relay use-client-side-address

Parameter	Description
use-client-side-address	Use the client side interface IP address as the source IP address for relayed DHCP packets.

Default By default, the server-side interface IP address is used as the source IP address of DHCP relayed packets.

Mode Global Configuration

Usage notes In most cases, there are filters placed between the DHCP relay and DHCP server which only allow DHCP packets from the client subnet to the server and back. This command allows you to configure the DHCP relay so that the relay will use the IP address of the interface **receiving** clients' DHCP requests to be used as the source IP address of the relayed DHCP packets.

Example To configure the client-side IP address as the source IP address of DHCP relayed packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-client-side-address
```

Output The following shows typical output.

Example output from show ip dhcp-relay

```
awplus#sh ip dhcp-relay
DHCP Relay Service is enabled
Use of client side address as source address is enabled
...
```

The second line of the display output shows the status of the client-side address being enabled as the source IP address.

Related commands [ip dhcp-relay server-address](#)

Command changes Version 5.4.9-0.7: command added

ip dhcp-relay use-dhcp-relay-ip

Overview Use this command to configure the device to use its own IP address in the "Server ID" option, when acting as a DHCP relay agent. By default, the device uses the address of the DHCP server instead.

You may find this command useful if the relay agent is configured to provide short lease times. This command can prevent the client from bypassing the relay agent and ending up with a longer lease from the server.

Use the **no** variant of this command to return to the default behavior.

Syntax `ip dhcp-relay use-dhcp-relay-ip`
`no ip dhcp-relay use-dhcp-relay-ip`

Default Disabled

Mode Global Configuration

Example To use the device's own IP address as the server ID, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-dhcp-relay-ip
```

To return to using the DHCP server's IP address as the server ID, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp-relay use-dhcp-relay-ip
```

Related commands [show ip dhcp-relay](#)

Command changes Version 5.5.5-0.1: command added

lease

Overview This command sets the expiration time for a leased address for the DHCP address pool you are configuring. The time set by the days, hours, minutes and seconds is cumulative. The minimum total lease time that can be configured is 20 seconds. The maximum total lease time that can be configured is 120 days.

Note that if you add a user-defined option 51 using the **option** command, then you will override any settings created with this command. Option 51 specifies a lease time of 1 day.

Use the **infinite** parameter to set the lease expiry time to infinite (leases never expire).

Use the **no** variant of this command to return the lease expiration time back to the default of one day.

Syntax lease <days> <hours> <minutes> [<seconds>]
lease infinite
no lease

Parameter	Description
<days>	The number of days, from 0 to 120, that the lease expiry time is configured for. Default: 1
<hours>	The number of hours, from 0 to 24, that the lease expiry time is configured for. Default: 0
<minutes>	The number of minutes, from 0 to 60, the lease expiry time is configured for. Default: 0
<seconds>	The number of seconds, from 0 to 60, the lease expiry time is configured for.
infinite	The lease never expires.

Default The default lease time is 1 day.

Mode DHCP Configuration

Examples To set the lease expiration time for address pool P2 to 35 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# lease 0 0 35
```

To set the lease expiration time for the address pool Nerv_Office to 1 day, 5 hours, and 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# lease 1 5 30
```

To set the lease expiration time for the address pool P3 to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P3
awplus(dhcp-config)# lease 0 0 0 20
```

To set the lease expiration time for the pool to never expire, use the command:

```
awplus(dhcp-config)# lease infinite
```

To return the lease expiration time to the default of one day, use the command:

```
awplus(dhcp-config)# no lease
```

Related commands [option](#)
[service dhcp-server](#)
[short-lease-threshold](#)

network (DHCP)

Overview This command sets the network (subnet) that the DHCP address pool applies to.

The **no** variant of this command removes the network (subnet) from the DHCP address pool.

Syntax `network {<ip-subnet-address/prefix-length>|<ip-subnet-address/mask>}`
`no network`

Parameter	Description
<code><ip-subnet-address/prefix-length></code>	The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.
<code><ip-subnet-address/mask></code>	The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation.

Mode DHCP Configuration

Usage notes This command will fail if it would make existing ranges invalid. For example, if they do not lie within the new network you are configuring.

The **no** variant of this command will fail if ranges still exist in the pool. You must remove all ranges in the pool before issuing a **no network** command to remove a network from the pool.

Examples To configure a network for the address pool P2, where the subnet is 192.0.2.5 and the mask is 255.255.255.0, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5/24
```

or you can use dotted decimal notation instead of slash notation for the subnet-mask:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5 255.255.255.0
```

Related commands [service dhcp-server](#)
[subnet-mask](#)

next-server

Overview This command sets the next server address for a DHCP server pool. It is the address of the next server that the client should use in its bootstrap process.

The **no** variant of this command removes the next server address from the DHCP address pool.

Syntax next-server <ip-address>
no next-server

Parameter	Description
<ip-address>	The server IP address, entered in dotted decimal notation.

Mode DHCP Configuration

Example To set the next-server address for the address pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# next-server 192.0.2.2
```

option

Overview This command adds a user-defined option to the DHCP address pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value. Options with an **ip** type can hold a list of IP addresses or masks (i.e. entries that have the A.B.C.D address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IP addresses.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes the specified user-defined option from the DHCP pool, or all user-defined options from the DHCP pool.

Syntax option [*<1-254>*|*<option-name>*] *<option-value>*
no option [*<1-254>*|*<option-name>*]

Parameter	Description
<i><1-254></i>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.
<i><option-name></i>	Option name associated with the option.
<i><option-value></i>	The option value. You must specify a value that is appropriate to the option type:
	hex A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	ip An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times.
	integer A number from 0 to 4294967295.
	flag A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.

Mode DHCP Configuration

Examples To add the ASCII-type option named `tftp-server-name` to the pool P2 and give the option the value `server1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool P2 and give the option the value `08af`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the command:

```
awplus(dhcp-config)# option 175 192.0.2.6
awplus(dhcp-config)# option 175 192.0.2.12
awplus(dhcp-config)# option 175 192.0.2.33
```

To add the option 179 to a pool, and give the option the value 123456, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the command:

```
awplus(dhcp-config)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the command:

```
awplus(dhcp-config)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

Related commands

- [dns-server](#)
- [ip dhcp option](#)
- [lease](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)

probe enable

Overview Use this command to enable lease probing for a DHCP pool. Probing is used by the DHCP server to check if an IP address it wants to lease to a client is already being used by another host.

The **no** variant of this command disables probing for a DHCP pool.

Syntax probe enable
no probe enable

Default Probing is enabled by default.

Mode DHCP Pool Configuration

Examples To enable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe enable
```

To disable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe enable
```

Related commands

- ip dhcp pool**
- probe packets**
- probe timeout**
- probe type**
- show ip dhcp pool**

probe packets

Overview Use this command to specify the number of packets sent for each lease probe. Lease probing is configured on a per-DHCP pool basis. When set to 0 probing is effectively disabled.

The **no** variant of this command sets the number of probe packets sent to the default of 5.

Syntax probe packets <0-10>
no probe packets

Parameter	Description
<0-10>	The number of probe packets sent.

Default The default is 5.

Mode DHCP Pool Configuration

Examples To set the number of probe packets to 2 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe packets 2
```

To set the number of probe packets to the default 5 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe packets
```

Related commands [probe enable](#)
[probe timeout](#)
[probe type](#)
[show ip dhcp pool](#)

probe timeout

Overview Use this command to set the timeout value in milliseconds that the server waits for a response after each probe packet is sent. Lease probing is configured on a per-DHCP pool basis.

The **no** variant of this command sets the probe timeout value to the default setting, 200 milliseconds.

Syntax probe timeout <50-5000>
no probe timeout

Parameter	Description
<50-5000>	Timeout interval in milliseconds.

Default The default timeout interval is 200 milliseconds.

Mode DHCP Pool Configuration

Examples To set the probe timeout value to 500 milliseconds for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe timeout 500
```

To set the probe timeout value for pool P2 to the default, 200 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe timeout
```

Related commands

- [probe enable](#)
- [probe packets](#)
- [probe type](#)
- [show ip dhcp pool](#)

probe type

Overview Use this command to set the probe type for a DHCP pool. The probe type specifies how the DHCP server checks whether an IP address is being used by other hosts, referred to as lease probing. If **arp** is specified, the server sends an ARP request to determine if an address is in use. If **ping** is specified, the server will send an ICMP Echo Request (ping).

The **no** variant of this command sets the probe type to the default setting, ping.

Syntax probe type {arp|ping}
no probe type

Parameter	Description
arp	Probe using ARP.
ping	Probe using ping.

Default The default probe type is ping.

Mode DHCP Pool Configuration

Examples To set the probe type to arp for the pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe type arp
```

To set the probe type for the pool P2 to the default, ping, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe type
```

Related commands

- [ip dhcp pool](#)
- [probe enable](#)
- [probe packets](#)
- [probe timeout](#)
- [show ip dhcp pool](#)

range

Overview This command adds an address range to the DHCP address pool you are configuring. The DHCP server responds to client requests received from the pool's network. It assigns an IP addresses within the specified range. The IP address range must lie within the network. You can add multiple address ranges and individual IP addresses for a DHCP pool by using this command multiple times.

The **no** variant of this command removes an address range from the DHCP pool. Use the **no range all** command to remove all address ranges from the DHCP pool.

Syntax `range <ip-address> [<ip-address>]`
`no range <ip-address> [<ip-address>]`
`no range all`

Parameter	Description
<code><ip-address></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
<hours>	The number of hours, from 0 to 24.
<minutes>	The number of minutes, from 0 to 60.

Default 1 minute.

Mode DHCP Configuration

Usage notes DHCP leases need to be backed up in NVS so that when the DHCP server reboots or goes through a power cycle it won't lose all the knowledge of these leases.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few seconds before their existing lease expires. This can happen for example, when mobile devices move in and out of a Wi-Fi zone or when Wi-Fi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

The **short-lease-threshold** command allows you to configure the threshold for a short lease, from 1 minute to 24 hours. Any lease less than the threshold is deemed to be a short lease and will NOT be backed up to NVS.

This is useful if you have:

- limited backup file space, and
- you don't need to restore leases after a device reboot or power cycle

Example To set the short lease threshold for address pool P2 to 40 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# short-lease-threshold 0 40
```

To set the short lease threshold for address pool Nerv_Office to 5 hours and 35 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# short-lease-threshold 5 35
```

To return the short lease threshold to the default of one minute, use the following commands:

```
awplus# configure terminal
awplus(config)# no short-lease-threshold
```

**Related
commands
Command
changes**

lease

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 The following shows typical output.

Example output from the show counter dhcp-client command

```
show counter dhcp-client

DHCPDISCOVER out      ..... 10
DHCPREQUEST out       ..... 34
DHCPDECLINE out       ..... 4
DHCPRELEASE out       ..... 0
DHCPOFFER in          ..... 22
DHCPACK in            ..... 18
DHCPNAK in            ..... 0
```

Parameters in the output of the show counter dhcp-client command

Parameter	Description
DHCPDISCOVER out	The number of DHCP Discover messages sent by the client.
DHCPREQUEST out	The number of DHCP Request messages sent by the client.
DHCPDECLINE out	The number of DHCP Decline messages sent by the client.
DHCPRELEASE out	The number of DHCP Release messages sent by the client.
DHCPOFFER in	The number of DHCP Offer messages received by the client.
DHCPACK in	The number of DHCP Acknowledgement messages received by the client.
DHCPNAK in	The number of DHCP Negative Acknowledgement messages received by the client.

Related [ip address dhcp commands](#)

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

Syntax (VRF-lite) show counter dhcp-relay [vrf <vrf-name>|global]

Parameter	Description
vrf	Display the output for a VRF instance
<vrf-name>	The name of the specific VRF instance.
global	Display the output for the Global VRF instance

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 The following shows typical output.

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
```

Example output from the show counter dhcp-relay command for VRF instance red

```
DHCP relay counters

[VRF red]
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
Option Insert Failed ..... 0
```

Parameter	Description
Requests In	The number of DHCP Request messages received from clients.
Replies In	The number of DHCP Reply messages received from servers.
Relayed To Server	The number of DHCP Request messages relayed to servers.
Relayed To Client	The number of DHCP Reply messages relayed to clients.

Parameter	Description
Out To Server Failed	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
Out To Client Failed	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
Invalid hlen	The number of incoming messages dropped due to an invalid hlen field.
Bogus giaddr	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.
Corrupt Agent Option	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
Missing Agent Option	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
Bad Circuit ID	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Missing Circuit ID	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface.

Parameter	Description
	Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Bad Remote ID	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Missing Remote ID	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Option Insert Failed	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: - the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the ip dhcp-relay information policy command. - there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.
Note that the following parameters are only used on the Global VRF instance when DHCPv6 is running	
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.

Parameter	Description
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

Syntax (VRF-lite) show counter dhcp-server [vrf <vrf-name>]

Parameter	Description
vrf	Display the output for a VRF instance
<vrf-name>	The name of the specific VRF instance.

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 The following shows typical output.

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

**Example
output from
the show
counter
dhcp-server
command
with VRFs
configured**

```
DHCP server counters[VRF: RED]
DHCPDISCOVER in          ..... 0
DHCPREQUEST in           ..... 7
DHCPDECLINE in           ..... 0
DHCPRELEASE in           ..... 0
DHCPINFORM in            ..... 0
DHCPOFFER out            ..... 0
DHCPACK out              ..... 7
DHCPNAK out              ..... 0
BOOTREQUEST in           ..... 0
BOOTREPLY out            ..... 0
DHCPLEASEQUERY in        ..... 0
DHCPLEASEUNKNOWN out     ..... 0
DHCPLEASEACTIVE out      ..... 0
DHCPLEASEUNASSIGNED out  ..... 0

[VRF: GREEN]
DHCPDISCOVER in          ..... 0
DHCPREQUEST in           ..... 7
DHCPDECLINE in           ..... 0
DHCPRELEASE in           ..... 0
DHCPINFORM in            ..... 0
DHCPOFFER out            ..... 0
DHCPACK out              ..... 7
DHCPNAK out              ..... 0
BOOTREQUEST in           ..... 0
BOOTREPLY out            ..... 0
DHCPLEASEQUERY in        ..... 0
DHCPLEASEUNKNOWN out     ..... 0
DHCPLEASEACTIVE out      ..... 0
DHCPLEASEUNASSIGNED out  ..... 0
```

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.
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 ip dhcp server statistics](#)

show dhcp lease

Overview This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

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

Syntax show dhcp lease [<interface>]

Parameter	Description
<interface>	Interface name to display DHCP lease details for.

Mode User Exec and Privileged Exec

Example To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for eth1, use the command:

```
awplus# show dhcp lease eth1
```

Output The following shows typical output.

Example output from the show dhcp lease eth1 command

Interface eth1	

IP Address:	192.168.22.4
Expires:	13 Mar 2022 20:10:19
Renew:	13 Mar 2022 18:37:06
Rebind:	13 Mar 2022 19:49:29
Server:	
Options:	
subnet-mask	255.255.255.0
routers	19.18.2.100,12.16.2.17
dhcp-lease-time	3600
dhcp-message-type	5
domain-name-servers	192.168.100.50,19.88.200.33
dhcp-server-identifier	192.168.22.1
domain-name	alliedtelesis.com

Related commands [ip address dhcp](#)

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>*]

Syntax (VRF-lite) show ip dhcp binding [vrf *<name>*] [*<ip-address>* | *<address-pool>*]

Parameter	Description
vrf	Display the output for a VRF instance
<i><name></i>	The name of the specific VRF instance.
<i><ip-address></i>	IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address.
<i><address-pool></i>	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 The following shows typical output.

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 Jun 2021 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 Jun 2021 14:58:41

Output (VRF-lite) The following shows typical output.

Example output from the show ip dhcp binding command for VRF instance red

[VRF: RED]Pool red_pool Network 192.168.1.0/24			
DHCP Client Entries			
IP Address	ClientId	Type	Expiry

192.168.1.2	0000.cd38.00bf	Dynamic	2 Jun 2021 13:38:470

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
<i><address-pool></i>	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 The following shows typical output.

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 msecs    [200]
Dynamic addresses:
  Total:       8
  Leased:      2
  Utilization: 25.0 %
Static host addresses:
  Total:       1
  Leased:      1
```

Parameters in the output of show ip dhcp pool

Parameter	Description
Pool	Name of the pool.
network	Subnet and mask length of the pool.
address ranges	Individual IP addresses and address ranges configured for the pool. The DHCP server can offer clients an IP address from within the specified ranges only. Any of these addresses that match an interface address on the device, or a static host address configured in the pool, will be automatically excluded from the range, and a message to this effect will appear beneath the range entry.
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.

Parameter	Description
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>]

Syntax (VRF-lite) show ip dhcp-relay [vrf <name>|global] [interface <interface-name>]

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.
vrf	Apply this command to a VRF instance.
<vrf-name>	The name of the VRF instance.
global	The Global VRF instance.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent’s configuration on the interface eth1, use the command:

```
awplus# show ip dhcp-relay interface eth1
```

Output The following shows typical output.

Example output from the show ip dhcp-relay command

```
DHCP Relay Service is enabled

eth1 is up, line protocol is up
Maximum hop count is 10
Maximum DHCP message length is 1400
DHCP Relay short lease time for IPv4 is 200 seconds
DHCP Relay short lease time for IPv6 are 2000/1900 (valid/
preferred) seconds
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
```

Output (VRF-lite) **Example output from the show ip dhcp-relay command applied for VRF instance red**

```
DHCP Relay Service is enabled

[VRF: red]
vlan2 is up, line protocol is up
Maximum hop count is 10
Maximum DHCP message length is 1400
Insertion of Relay Agent Option is enabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay Information policy is to replace existing relay agent
information
List of servers : 192.168.1.3
```

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

Syntax (VRF-lite) show ip dhcp server statistics [vrf <name>]

Parameter	Description
vrf	Display the output for a VRF instance.
<name>	The name of the specific VRF instance.

Mode User Exec and Privileged Exec

Example To display the server statistics, use the command:

```
awplus# show ip dhcp server statistics
```

Output The following shows typical output.

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
```

Example output from the show ip dhcp server statistics command for VRF instance red

```
DHCP relay counters
[VRF: RED]
DHCPDISCOVER in      ..... 0
DHCPREQUEST in       ..... 7
DHCPDECLINE in        ..... 0
DHCPRELEASE in        ..... 0
DHCPINFORM in         ..... 0
DHCPOFFER out        ..... 0
DHCPACK out           ..... 7
DHCPNAK out           ..... 0
BOOTREQUEST in        ..... 0
BOOTREPLY out         ..... 0
DHCPLEASEQUERY in     ..... 0
DHCPLEASEUNKNOWN out  ..... 0
DHCPLEASEACTIVE out   ..... 0
DHCPLEASEUNASSIGNED out ..... 0
```

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.

Parameter	Description
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](#)

Command changes Version 5.5.1-1.1: **vrf** <name> parameter added

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 The following shows typical output.

Example output from the show ip dhcp server summary command

```
DHCP Server service is enabled
DHCP Server is running
BOOTP ignore is disabled
DHCP leasequery support is disabled
DHCP server is globally authoritative
DHCP subscriber-id substitution for client-id is not enabled
Pool list: p2
```

Related commands [ip dhcp leasequery enable](#)
[ip dhcp pool](#)
[service dhcp-server](#)

subnet-mask

Overview This command sets the subnet mask option for a DHCP address pool you are configuring. Use this command to specify the client's subnet mask as defined in RFC 950. This sets the subnet details using the pre-defined option 1. Note that if you create a user-defined option 1 using the **option** command, then you will override any settings created with this command. If you do not specify a subnet mask using this command, then the pool's network mask (specified using the **next-server** command) is applied.

The **no** variant of this command removes a subnet mask option from a DHCP pool. The pool reverts to using the pool's network mask.

Syntax subnet-mask <mask>
no subnet-mask

Parameter	Description
<mask>	Valid IPv4 subnet mask, in dotted decimal notation.

Mode DHCP Configuration

Examples To set the subnet mask option to 255 . 255 . 255 . 0 for DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

Related commands

- default-router**
- dns-server**
- domain-name**
- next-server**
- option**
- service dhcp-server**
- show ip dhcp pool**

vrf

Overview Use this command to add a VRF name to a DHCP server's address pool. This enables the DHCP server to become VRF-aware and allocate IP addresses which are the same as other pools.

One of the benefits of using this command is that it allows you to share DHCP leases across multiple isolated networks.

Use the **no** variant of this command to remove a VRF name from the DHCP server pool.

Syntax `vrf <vrf-name>`
`no vrf`

Parameter	Description
<code><vrf-name></code>	The name of the specific VRF instance.

Default Global VRF

Mode DHCP Configuration

Usage notes You need to enter this **vrf** command before entering the **network (DHCP)** and **range** address commands.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

Example To add the VRF name 'red' to the DHCP pool named 'P1', use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P1
awplus(dhcp-config)# vrf red
```

To remove a VRF name from the DHCP pool named 'P1', use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P1
awplus(dhcp-config)# no vrf
```

Related commands [network \(DHCP\)](#)
[range](#)
[show ip dhcp pool](#)

Command changes Version 5.5.1-1.1: command added

32

DHCP for IPv6 (DHCPv6) Commands

- Contents**
- **Introduction** on page 1688
 - **address prefix** on page 1689
 - **address range** on page 1691
 - **clear counter ipv6 dhcp-client** on page 1693
 - **clear counter ipv6 dhcp-server** on page 1694
 - **clear ipv6 dhcp binding** on page 1695
 - **clear ipv6 dhcp client** on page 1697
 - **dns-server (DHCPv6)** on page 1698
 - **domain-name (DHCPv6)** on page 1700
 - **ip dhcp-relay agent-option** on page 1701
 - **ip dhcp-relay agent-option checking** on page 1703
 - **ip dhcp-relay agent-option remote-id** on page 1704
 - **ip dhcp-relay information policy** on page 1706
 - **ip dhcp-relay maxhops** on page 1708
 - **ip dhcp-relay max-message-length** on page 1709
 - **ip dhcp-relay server-address** on page 1711
 - **ip dhcp-relay short-lease-ipv6** on page 1713
 - **ipv6 address (DHCPv6 PD)** on page 1715
 - **ipv6 address dhcp** on page 1717
 - **ipv6 dhcp client pd** on page 1719
 - **ipv6 dhcp option** on page 1721
 - **ipv6 dhcp pool** on page 1724
 - **ipv6 dhcp server** on page 1726
 - **ipv6 local pool** on page 1728
 - **ipv6 nd prefix (DHCPv6)** on page 1730
 - **link-address** on page 1733
 - **option (DHCPv6)** on page 1735
 - **prefix-delegation pool** on page 1738
 - **service dhcp-relay** on page 1740
 - **show counter dhcp-relay** on page 1741
 - **show counter ipv6 dhcp-client** on page 1746
 - **show counter ipv6 dhcp-server** on page 1748
 - **show ip dhcp-relay** on page 1751
 - **show ipv6 dhcp** on page 1753
 - **show ipv6 dhcp binding** on page 1754
 - **show ipv6 dhcp interface** on page 1758
 - **show ipv6 dhcp pool** on page 1760

- [**sntp address**](#) on page 1762

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.*

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
<ipv6-prefix/prefix-length>	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.
lifetime	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.
<valid-time>	Specify a valid lifetime in seconds in the range <5-315360000>. The default valid lifetime is 2592000 seconds.
infinite	Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.
<preferred-time>	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><first-ipv6-address></code>	Specify the first IPv6 address of the IPv6 address range, in hexadecimal notation in the format X:X::X:X.
<code><last-ipv6-address></code>	Specify the last IPv6 address of the IPv6 address range, in hexadecimal notation in the format X:X::X:X.
<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. 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><valid-time></code>	Specify a valid lifetime in seconds in the range <5-31536000>. 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><preferred-time></code>	Specify a preferred lifetime in seconds in the range <5-31536000>. 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
ipv6 <prefix>	Optional. Specify the IPv6 prefix of the DHCPv6 client, in hexadecimal notation in the format X:X::X:X.
duid <DUID>	Specify the DUID (DHCPv6 unique ID) of the DHCPv6 client.
all	All DHCPv6 bindings.
pool <name>	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 The following shows typical output.

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><interface></code>	Specify the interface name to restart a DHCPv6 client on.

Mode Privileged Exec

Example To restart a DHCPv6 client on interface eth1, use the following command:

```
awplus# clear ipv6 dhcp client eth1
```

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)**, 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><ipv6-address></code>	Specify an IPv6 address of the DNS server, in hexadecimal notation in the format X:X::X:X. This parameter is required when adding a DNS server to the DHCPv6 address pool. All DNS servers are removed from the DHCPv6 pool if you enter the <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
<domain-name>	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)**, 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: *ip dhcp-relay agent-optionip dhcp-relay information policy*

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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 relay agent listening on eth1 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To make the relay agent listening on eth1 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related commands **ip dhcp-relay agent-option**
ip dhcp-relay agent-option remote-id
ip dhcp-relay information policy
service dhcp-relay

ip dhcp-relay agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

Syntax ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed.

Default The Remote ID is set to the device's MAC address by default.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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: *ip dhcp-relay agent-optionip dhcp-relay information policy*

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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Examples To make the DHCP Relay Agent listening on eth1 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Example To set the maximum number of hops to 5 for packets received on interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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: [ip dhcp-relay agent-option](#)

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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
<code><ipv4-address></code>	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.
<code><ipv6-address></code>	Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.
<code><server-interface></code>	Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 eth1 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

DHCP for IPv4

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1
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 eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

Examples: To enable the DHCP Relay Agent on your device to relay DHCP packets on interface eth1.2 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4, use the commands:

DHCPv6

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1.2
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4 from the list of servers available to the DHCP Relay Agent on interface eth1.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

Example: To disable DHCP relay on eth1, use the commands:

disabling DHCP relay

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip dhcp-relay
```

Related commands [service dhcp-relay](#)

ip dhcp-relay short-lease-ipv6

- Overview** Use this command to reduce the amount of time an IPv6 address is assigned to a client device.
- Long lease times can cause issues in dynamic networks where client devices frequently move between segments, such as VLANs. These device may retain an outdated IP address from its previous VLAN, disrupting communication.
- This command is particularly useful in networks with a high turnover of devices or in environments where IP addresses are scarce.
- Use the **no** variant of this command to remove the short lease time configuration.

Syntax `ip dhcp-relay short-lease-ipv6 [<20-3600> <20-3600>]`
`no ip dhcp-relay short-lease-ipv6`

Parameter	Description
<20-3600>	The valid lease time for IPv6 DHCP relay in seconds.
<20-3600>	The preferred lease time for IPv6 DHCP relay in seconds.

Default Not set

Mode Interface Configuration

- Usage notes** The preferred lease time (the second parameter) must be less than the valid lease time (the first parameter).
- **Preferred lease time:** Indicates when preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.
 - **Valid lease time:** Indicates when IPv6 addresses or prefixes must be abandoned. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires.

Example To configure a DHCP Relay on interface vlan1 with a valid lease time of 2000 seconds, and a preferred lease time of 1000 seconds for IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease-ipv6 2000 1000
```

Related commands [show ip dhcp-relay](#)

Command changes Version 5.5.4-2.1: command added

ipv6 address (DHCPv6 PD)

Overview Use this command 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><ipv6-prefix-name></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><ipv6-addr/prefix-length></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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 assign the IPv6 address 2001:0db8::a2/48 to the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:0db8::a2/48
```

To remove the IPv6 address 2001:0db8::a2/48 from the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 address 2001:0db8::a2/48
```

To assign the **eui64** derived address in the prefix 2001:0db8::/64 to interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:0db8::/64 eui64
```

To remove the **eui64** derived address in the prefix 2001:0db8::/64 from interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 address 2001:0db8::/64 eui64
```

To configure a PD prefix named 'prefix1' on interface eth1 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 eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1::1/64
```

Related commands

- [ipv6 dhcp client pd](#)
- [ipv6 dhcp pool](#)
- [ipv6 local pool](#)
- [ipv6 nd prefix \(DHCPv6\)](#)
- [prefix-delegation pool](#)
- [show ipv6 dhcp binding](#)
- [show ipv6 interface](#)
- [show ipv6 route](#)
- [show running-config](#)

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`

Parameter	Description
default-route-to-server	Allow the automatic configuration of a default route to the DHCPv6 server. This option is not enabled by default when you enable the DHCP client on an interface.

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes Use the **default-route-to-server** option to allow the automatic configuration of a default route to the DHCPv6 server. Note that this option is not enabled by default when you enable the DHCP client on an interface.

Examples To set the interface eth1 to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface eth1 from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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><prefix-name></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><default-route-to-server></code>	Specify the default route to the DHCP server

Mode Interface Configuration for Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 my-prefix-name on the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd my-prefix-name
```

To disable prefix delegation on the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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". Default: no default
<option-type>	The option value. You must specify a value that is appropriate to the option type:
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: true, on, or enabled will set the flag. false, off or disabled will unset the flag.

Mode Global Configuration

Examples To define a user-defined ASCII string option as option 66, without a name, use the 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><DHCPv6-poolname></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 ipv6 dhcp pool command. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

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 interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 dhcp server P2
```

To disable the DHCPv6 server on interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 dhcp server
```

Related **ipv6 dhcp pool**
commands **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><DHCPv6-poolname></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><delegated-prefix-name></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><ipv6-prefix/prefix-length></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><assigned-length></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 an interface.

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><ipv6-prefix-name></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><ipv6-prefix/length></code>	The IPv6 prefix and prefix length advertised on the router advertisement message sent from the device. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<code><valid-lifetime></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><valid-lifetime></code> parameter applies an infinite valid lifetime.
<code><preferred-lifetime></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><preferred-lifetime></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 Eth, WWAN, and bridge interfaces and 802.1Q sub-interfaces.

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 interface eth1, and advertises the DHCPv6 prefix name prefix1 and the IPv6 address prefix of 2001:0db8::/32.

```
awplus# configure terminal
awplus(config)# interface eth1
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 interface eth1, so the address prefix of 2001:0db8::/32 is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/32
```

The following example removes all prefix names and prefixes from interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
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
<ipv6-prefix/prefix-length>	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 **dns-server (DHCPv6)**
commands **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><DHCPv6-poolname></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. 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><valid-time></code>	Specify a valid lifetime in seconds in the range <5-315360000>.
<code>infinite</code>	Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.
<code><preferred-time></code>	Specify a valid lifetime in seconds in the range <5-315360000>.

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

Syntax (VRF-lite) show counter dhcp-relay [vrf <vrf-name>|global]

Parameter	Description
vrf	Display the output for a VRF instance
<vrf-name>	The name of the specific VRF instance.
global	Display the output for the Global VRF instance

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 The following shows typical output.

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
```

Example output from the show counter dhcp-relay command for VRF instance red

```
DHCP relay counters

[VRF red]
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
Option Insert Failed ..... 0
```

Parameter	Description
Requests In	The number of DHCP Request messages received from clients.
Replies In	The number of DHCP Reply messages received from servers.
Relayed To Server	The number of DHCP Request messages relayed to servers.
Relayed To Client	The number of DHCP Reply messages relayed to clients.

Parameter	Description
Out To Server Failed	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
Out To Client Failed	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
Invalid hlen	The number of incoming messages dropped due to an invalid hlen field.
Bogus giaddr	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.
Corrupt Agent Option	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
Missing Agent Option	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
Bad Circuit ID	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Missing Circuit ID	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface.

Parameter	Description
	Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Bad Remote ID	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Missing Remote ID	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
Option Insert Failed	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: - the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the ip dhcp-relay information policy command. - there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.
Note that the following parameters are only used on the Global VRF instance when DHCPv6 is running	
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.

Parameter	Description
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 The following shows typical output.

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
```

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.
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 The following shows typical output.

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
RELAY FORWARD in         ..... 0
LEASEQUERY in             ..... 0
DHCPv4 QUERY in           ..... 0
```

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.
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
RELAY FORWARD in	Displays the count of Relay forward in messages received by the DHCPv6 server

Parameter	Description
LEASEQUERY in	Displays the count of LEASE QUERY messages received by the DHCPv6 server
DHCPv4 QUERY in	Displays the count of DHCPv4 QUERY 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>]

Syntax (VRF-lite) show ip dhcp-relay [vrf <name>|global] [interface <interface-name>]

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.
vrf	Apply this command to a VRF instance.
<vrf-name>	The name of the VRF instance.
global	The Global VRF instance.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent’s configuration on the interface eth1, use the command:

```
awplus# show ip dhcp-relay interface eth1
```

Output The following shows typical output.

Example output from the show ip dhcp-relay command

```
DHCP Relay Service is enabled

eth1 is up, line protocol is up
Maximum hop count is 10
Maximum DHCP message length is 1400
DHCP Relay short lease time for IPv4 is 200 seconds
DHCP Relay short lease time for IPv6 are 2000/1900 (valid/
preferred) seconds
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
```

Output (VRF-lite) **Example output from the show ip dhcp-relay command applied for VRF instance red**

```
DHCP Relay Service is enabled

[VRF: red]
vlan2 is up, line protocol is up
Maximum hop count is 10
Maximum DHCP message length is 1400
Insertion of Relay Agent Option is enabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay Information policy is to replace existing relay agent
information
List of servers : 192.168.1.3
```

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 The following shows typical output.

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 summary 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 The following shows typical output.

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

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 The following shows typical output.

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
```

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.

Parameter	Description
	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.
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
```

To display DHCPv6 information for interface eth1, use the command:

```
awplus# show ipv6 dhcp interface eth1
```

Output The following shows typical output.

Example output from the show ipv6 dhcp interface command

```
awplus# show ipv6 dhcp interface
eth1 is in client mode
  Address 1001::3c0:1
    preferred lifetime 9000, valid lifetime 5000
    starts at 20 Jan 2021 09:21:35
    expires at 20 Jan 2021 10:25:32
```

**Example
output from
the show
ipv6 dhcp
interface
command
for a specific
interface**

```
awplus# show ipv6 dhcp interface eth1
eth1 is in client (Prefix-Delegation) mode
Prefix name pd1
    prefix 2002:0:3c0::/42
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2021 09:21:33
    expires at 19 Sep 2021 09:21:33
```

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
<i><DHCPv6-address-pool-name></i>	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 The following shows typical output.

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)
```

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.
Address Lifetime	Valid and preferred lifetimes to the DHCPv6 pool. 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.
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. SNTP is Simple Network Time Protocol.

Use the **no** variant of this command to remove an SNTP Server IPv6 address from a DHCPv6 Server pool.

Syntax sntp address {<ipv6-address>|interface <server-interface>}
no sntp address {<ipv6-address>|interface <server-interface>}

Parameter	Description
<ipv6-address>	Specify an SNTP Server IPv6 address, in hexadecimal notation in the format X:X::X:X.
interface <server- interface>	Source the IPv6 address from an interface.

Mode DHCPv6 Configuration

Examples To add an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# sntp address 2001:0db8::/32
```

To remove an SNTP Server IPv6 address of 2001:0db8::/32 from the DHCPv6 pool named P2, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no sntp address 2001:0db8::/32
```

To add the SNTP Server that has a dynamic address source of vlan10 to the DHCPv6 pool named P2, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# sntp address interface vlan10
```

Related commands

- dns-server (DHCPv6)**
- domain-name (DHCPv6)**
- option (DHCPv6)**
- show ipv6 dhcp pool**

33

Download Portal Commands

- Contents**
- **Introduction** on page 1764
 - **aaa authentication download-portal** on page 1765
 - **download-portal** on page 1767
 - **download-portal reload** on page 1768
 - **enable (download-portal)** on page 1769
 - **file (download-portal)** on page 1770
 - **http listen** on page 1772
 - **http secure-listen** on page 1774
 - **secure-listen (download-portal)** on page 1776
 - **show download-portal** on page 1778
 - **uri (download-portal)** on page 1779

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Download Portal.

The Download Portal provides a mechanism for administrators to offer resources to network users, protected by authentication. The resources could include software installers and setup guidelines, for example a remote access client along with setup instructions.

For more information, see the [Download Portal Feature Overview and Configuration Guide](#).

aaa authentication download-portal

Overview Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

Syntax `aaa authentication download-portal default group [<group-name>|radius|ldap]`

`no aaa authentication download-portal default`

Parameter	Description
<code><group-name></code>	Server group name.
<code>radius</code>	Use all RADIUS servers
<code>ldap</code>	Use all LDAP servers

Default Authentication for Download Portal clients is disabled by default.

Mode Global Configuration

Usage notes There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the **radius-server host** command.
- **group ldap:** use all LDAP servers configured with the **ldap-server** command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the **aaa group server** command.

Example To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default group
ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default group
my_group
```

Note: This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

Related commands [aaa group server](#)
[download-portal](#)

Command changes Version 5.5.4-0: command added

download-portal

Overview Use this command to enter Download Portal configuration mode.

Use the **no** variant of this command to remove all Download Portal configuration.

Syntax download-portal
no download-portal

Mode Global Configuration

Usage notes The Download Portal enables AlliedWare Plus administrators to provide resources to authenticated network users. These resources may include software installers and setup guidelines, such as a remote access client with accompanying instructions. The resources offered are curated and configured by AlliedWare Plus administrators.

Example To enter Download Portal configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)#
```

To remove all Download Portal configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no download-portal
awplus(config)#
```

Related commands [enable \(download-portal\)](#)
[secure-listen \(download-portal\)](#)
[file \(download-portal\)](#)
[uri \(download-portal\)](#)
[show download-portal](#)

Command changes Version 5.5.4-0: command added

download-portal reload

Overview Use this command to reload the Download Portal which will recreate the Download Portal page.

Syntax download-portal reload

Mode Privileged Exec

Usage Notes This is necessary if your device supports external media, such as a USB or SD card, and files are configured from the external media while the external media is not plugged in. When the external media is plugged in the Download Portal page is not automatically reloaded so the files will not appear. Use this command to force a reload.

Example To reload the Download Portal page, use the command:
awplus# download-portal reload

Related commands [download-portal](#)

Command changes Version 5.5.4-0: command added

enable (download-portal)

Overview Use this command to enable the Download Portal.
Use the **no** variant of this command to disable the Download Portal.

Syntax enable
no enable

Default Not enabled.

Mode Download Portal Configuration

Example To enable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# enable
```

To disable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no enable
```

Related commands [download-portal](#)

Command changes Version 5.5.4-0: command added

file (download-portal)

Overview Use this command to configure a file that will be displayed in the Download Portal page.

Use the **no** variant of this command to remove a file from the Download Portal page.

Syntax file <file-path> [sha256sum <hex-string>] [description <file-description>]
no file <file-path> [sha256sum <hex-string>] [description <file-description>]

Parameter	Description
<file-path>	The path to the file to be made available in the Download Portal. This file must be present in Flash, USB, or SD card storage.
sha256sum	Optionally, provide the sha256sum of the file. If configured, then this is checked against the file and if it does not match, then it is not displayed on the Download Portal page.
description	Optionally provide a description for the file to be presented to the user accessing the Download Portal page

Mode Download Portal Configuration

- Usage notes** The file path must be specific, such as starts with "flash:/"(Flash), "usb:/"(USB), or "card:/"(SDcard):
- If the file path is incorrect, the configured file does not show on the Download Portal page.
 - The checksum of the file is optional, but if the configured value is not matched, the file will not be shown on the Download Portal page.
 - Description is optional, it helps users understand what the file is about.

Example To configure files for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# file flash:/staff.txt sha256sum
a1bed1569bef6b9f8958bf8993ef53bf7c2f62a1833fe41f14 description
"Staff List"
awplus(config-download-portal)# file usb:/3g.bin description "3G
file for testing purpose"
awplus(config-download-portal)# file card:/default.cfg
description "Default Configuration File"
```

To remove a file from the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no file flash:/staff.txt
```

Related commands [download-portal](#)
[download-portal reload](#)

Command changes Version 5.5.4-0: command added

http listen

Overview Use this command to configure the HTTP service to stop listening on all addresses and, instead, listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTP service was listening on.

Syntax `http listen {<ip-address>|<ipv6-address>} <1-65535>`
`no http listen {<ip-address>|<ipv6-address>} <1-65535>`

Parameter	Description
<code><ip-address></code>	Specify the IPv4 address to listen on for HTTP connections, entered in the form A.B.C.D.
<code><ipv6-address></code>	Specify the IPv6 address to listen on for HTTP connections, entered in the form X:X::X:X.
<code><1-65535></code>	The TCP port to listen on for HTTP connections.

Mode Privileged Exec

Usage notes AlliedWare Plus devices are configured by default to allow access to the HTTP service using the default HTTP port 80 from any configured address on the device.

However, you can configure the HTTP service to listen on a specific address and port by using the **http listen** command in combination with the **http port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two commands helps to ensure the AlliedWare Plus HTTP service is only reachable on a particular interface. It is recommended that the AlliedWare Plus HTTP service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

Example To disable the HTTP service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http port none
awplus(config)# http listen 192.168.1.1 10080
```

To remove an address and port that the HTTP service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http listen 192.168.1.1 10080
```


Related [download-portal](#)
commands

Command Version 5.5.4-0: command added
changes

http secure-listen

Overview Use this command to configure the HTTPS service to stop listening on all addresses and instead listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTPS service was listening on.

Syntax `http secure-listen {<ip-address>|<ipv6-address>} <1-65535>`
`no http secure-listen {<ip-address>|<ipv6-address>} <1-65535>`

Parameter	Description
<ip-address>	Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.
<ipv6-address>	Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X.
<1-65535>	The TCP port to listen on for HTTPS connections.

Mode Privileged Exec

Usage notes By default, AlliedWare Plus devices are configured to allow access to the HTTPS service on the default HTTPS port 443 from any configured address on the device.

However, you can configure the HTTPS service to listen on a specific address and port by using the **http secure-listen** command in combination with the **http secure-port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two 'http' commands help ensure the AlliedWare Plus HTTPS service is only reachable on a particular interface. We recommend that the AlliedWare Plus HTTPS service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

Example To stop the HTTPS service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http secure-port none
awplus(config)# http secure-listen 192.168.1.1 10443
```

To remove an address and port that the HTTPS service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http secure-listen 192.168.1.1 10080
```

Related [download-portal](#)
commands

Command Version 5.5.4-0: command added
changes

secure-listen (download-portal)

Overview Use this command to add an address and port for the Download Portal to listen on for HTTPS connections.

Use the **no** variant of this command to remove a secure listen address and port.

Syntax secure-listen {<ip-address>|<ipv6-address>} <1-65535>
no secure-listen {<ip-address>|<ipv6-address>} <1-65535>

Parameter	Description
<ip-address>	Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.
<ipv6-address>	Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X.
<1-65535>	TCP port to listen on for HTTPS connections.

Mode Download Portal Configuration

Usage notes By default, the Download Portal cannot be accessed because it is not listening on any port for HTTP or HTTPS client connections. The **secure-listen** command must be configured to set the addresses and ports that the Download Portal HTTP service will listen on for clients connections. The IP specified must be configured on an interface.

It is recommended that the firewall rules are configured to ensure that the Download Portal is only reachable by clients that you expect.

Example To add an address and port for the Download Portal to listen on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# secure-listen 192.168.2.45 10443
```

To remove an address and port that the Download Portal was listening on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no secure-listen 192.168.2.45
10443
```

Related commands [download-portal](#)

Command changes Version 5.5.4-0: command added

show download-portal

Overview Use this command to show the current status of the Download Portal and display the total configured files and URIs (Uniform Resource Identifiers).

Syntax show download-portal

Mode Privileged Exec

Example To show the number of configured URIs and files for the Download Portal, use the command:

```
awplus# show download-portal
```

Output The following shows typical output.

Example output from show download-portal

```
awplus#show download-portal
Status: Enabled
Files: 2
Secure-listen  Addresses:

192.168.1.15:8443
```

Related commands [download-portal](#)

Command changes Version 5.5.4-0: command added

uri (download-portal)

Overview Use this command to configure a URI (Uniform Resource Identifier) that links to an external resource to be displayed on the Download Portal page.

Use the **no** variant of this command to remove the URI link from the Download Portal page.

Syntax uri <uri-link> [description <uri-description>]
no uri <uri-link>

Parameter	Description
<uri-link>	The URI link to be displayed. It must have a protocol prefix, such as: "https://" or "mailto://"
<uri-description>	Optionally provide a description for the URI to be presented to the user on the Download Portal page.

Mode Download Portal Configuration

Example To set a URI with a description for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# uri https://alliedtelesis.com
description Company Page
```

To remove a URI for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no uri https://alliedtelesis.com
```

Related commands [download-portal](#)

Command changes Version 5.5.4-0: command added

34

NTP Commands

- Contents**
- **Introduction** on page 1781
 - **ntp authentication-key** on page 1782
 - **ntp broadcastdelay** on page 1783
 - **ntp master** on page 1784
 - **ntp peer** on page 1785
 - **ntp rate-limit** on page 1787
 - **ntp restrict** on page 1788
 - **ntp server** on page 1790
 - **ntp source** on page 1792
 - **show ntp associations** on page 1794
 - **show ntp counters** on page 1797
 - **show ntp counters associations** on page 1798
 - **show ntp status** on page 1799

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](#).

ntp authentication-key

Overview This command defines each of the authentication keys. Each key has a key number, a type (MD5 or SHA1), and a value.

The **no** variant of this disables the authentication key.

Syntax ntp authentication-key <keynumber> md5 <key-string> [trusted]
ntp authentication-key <keynumber> sha1 <key-string> [trusted]
no ntp authentication-key <keynumber>

Parameter	Description
<keynumber>	<1-4294967295> An identification number for the key.
md5	Define an MD5 key.
sha1	Define an SHA1 key.
<key-string>	The authentication key. For SHA1, this is a 20 hexadecimal character string. For MD5, this is a string of up to 31 ASCII characters.
trusted	Add this key to the list of authentication keys that this server trusts.

Mode Global Configuration

Examples To define an MD5 authentication key number 134343 and a key value 'mystring', use the commands:

```
awplus# configure terminal  
awplus(config)# ntp authentication-key 134343 md5 mystring
```

To disable the authentication key number 134343 with the key value 'mystring', use the commands:

```
awplus# configure terminal  
awplus(config)# no ntp authentication-key 134343
```

Command changes Version 5.4.9-2.1 sha1-encrypted parameter added.

ntp broadcastdelay

Overview Use this command to set the estimated round-trip delay for broadcast packets.

Use the **no** variant of this command to reset the round-trip delay for broadcast packets to the default offset of 0 microseconds.

Syntax ntp broadcastdelay <delay>
no ntp broadcastdelay

Parameter	Description
<delay>	<1-999999> The broadcast delay in microseconds.

Default 0 microsecond offset, which can only be applied with the **no** variant of this command.

Mode Global Configuration

Examples To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:

```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```

To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:

```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```

ntp master

Overview Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source.

Use the **no** variant of this command to stop the device being the designated NTP server.

Syntax ntp master [<stratum>]
no ntp master

Parameter	Description
<stratum>	<1-15> The stratum number defines the configured level that is set for this master within the NTP hierarchy. The default stratum number is 12.

Mode Global Configuration

Usage notes The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: www.ntp.org

Examples To stop the device from being the designated NTP server, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2, use the commands:

```
awplus# configure terminal
awplus(config)# ntp master 2
```

ntp peer

Overview Use this command to configure an NTP peer association. An NTP association is a peer association if this system is willing to either synchronize to the other system, or allow the other system to synchronize to it.

Use the **no** variant of this command to remove the configured NTP peer association.

Syntax ntp peer {<peeraddress>|<peername>} [prefer] [key <key>]
[version <version>]
no ntp peer {<peeraddress>|<peername>}

Syntax (VRF-lite) ntp peer {<peeraddress>} [vrf <vrf-name>] [prefer] [key <key>]
[version <version>]
no ntp peer {<peeraddress>}

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.
vrf <vrf-name>	Specify the VRF the peer runs in. Note: this does not work when a hostname is used. It only works if an IP address is specified.
key <key>	<1-4294967295> Configure the peer authentication key.
version <version>	<1-4> Configure for this NTP version.

Mode Global Configuration

Examples To set an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

To set an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

To set the preferred peer to be IPv4 192.0.2.23 and the version to 4, with the authentication key '1234', use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
```

Examples (VRF-lite) To configure an NTP peer association for the peer with IP address 192.0.5.27, on the VRF 'red', use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.5.27 vrf red
```

To remove an NTP peer association for the peer with IP address 192.0.5.27, on the VRF 'red', use the commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.5.27
```

Related commands [ntp server](#)
[ntp source](#)

Command changes Version 5.5.2-2.1: VRF parameter added

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
Command changes

ntp restrict
Version 5.4.8-1.1: command added

ntp restrict

Overview Use this command to configure a restriction (allow or deny) on NTP packets or NTP functionality for a specific host/network or all hosts of a given IP family.

This means you can control host access to NTP service and NTP server status queries.

Use the **no** variant of this command to remove a restriction from one or more hosts.

Syntax

```
ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>}
{allow|deny}

ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>} query {allow|deny}

ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>} serve {allow|deny}

no ntp restrict {default-v4|default-v6|<host-address>|<host-subnet>}
```

Parameter	Description
default-v4	Apply this restriction to all IPv4 hosts.
default-v6	Apply this restriction to all IPv6 hosts.
<host-address>	Apply this restriction to the specified IPv4 or IPv6 host. Enter an IPv4 address in the format A.B.C.D. Enter an IPv6 address in the format X:X::X:X.
<host-subnet>	Apply this restriction to the specified IPv4 subnet or IPv6 prefix. Enter an IPv4 subnet in the format A.B.C.D/M. Enter an IPv6 prefix in the format X:X::X/X.
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
Command changes

ntp rate-limit

Version 5.4.8-1.1: command added

ntp server

Overview Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa. You can configure an NTP server association by hostname or IP address.

Use the **no** variant of this command to remove the configured NTP server.

Syntax `ntp server {<serveraddress>|<servername>} [prefer] [key <key>]
[version <version>]
no ntp server {<serveraddress>|<servername>}`

Syntax (VRF-lite) `ntp server <serveraddress> [vrf <vrf-name>] [prefer] [key <key>]
[version <version>]
no ntp server <serveraddress>`

Parameter	Description
<serveraddress>	Specify the IP address of the peer, entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X.X for an IPv6 address.
<servername>	Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.
prefer	Prefer this server when possible.
key <key>	Configure the server authentication key from the range 1 to 4294967295.
version <version>	Configure for this NTP version from the range 1 to 4.
vrf <vrf-name>	Specify a VRF for the server to run in. Note that this does not work when a hostname is used. It only works if an IP address is specified.

Mode Global Configuration

Examples To obtain the time by synchronizing with the server at 192.0.1.23, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
```

To obtain the time by synchronizing with the server at 192.0.1.23, and specify that this is the best server to use, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23 prefer
```

To obtain the time by synchronizing with the server at 2001:0db8:010e::2, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
```

To obtain the time by synchronizing with the server at 2001:0db8:010e::2, and specify that this is the best server to use, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2 prefer
```

To stop using the time server at 2001:0db8:010e::2, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

Examples (VRF-lite) To configure an NTP server association for the server with IP address 192.0.5.27, on the VRF red, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.5.27 vrf red
```

To remove an NTP server association for the server with an IPv4 address of 192.0.5.27, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.5.27
```

Related commands [ntp peer](#)
[ntp source](#)

Command changes Version 5.5.2-2.1: VRF parameter added

ntp source

Overview Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Note that you cannot use this command when using AMF (Allied Telesis Management Framework).

Use the **no** variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

Syntax ntp source <source-address>
no ntp source

Parameter	Description
<source-address>	Specify the IP address of the NTP source interface, entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X.X for an IPv6 address.

Default An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or invalid.

Mode Global Configuration

Usage notes Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server is determined by the **ntp peer** and **ntp server** commands.

Examples To configure the NTP source interface with the IPv4 address 192.0.2.23, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.2.23
```

To configure the NTP source interface with the IPv6 address 2001:0db8:010e::2, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 2001:0db8:010e::2
```

To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp source
```

Related commands [ntp peer](#)
[ntp server](#)

show ntp associations

Overview Use this command to display the status of NTP associations.

Syntax show ntp associations

Mode User Exec and Privileged Exec

Example To display the status of NTP associations, use the command:

```
awplus# show ntp associations
```

Output The following shows typical output.

Output from 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									

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.
st	The stratum, which is the number of hops between the server and the accurate time source such as an atomic clock.
t	Type, one of: u: unicast or multicast client b: broadcast or multicast client! s: symmetric peer A: multicast server B: broadcast server M: multicast server

Parameter	Description
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
```

```
awplus#show ntp counters
Server Received      4
Server Dropped      0
Client Sent         90
Client Received      76
Client Valid Received 76
```

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 The following shows typical output.

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
```

Parameters in the output from show ntp counters associations

Parameter	Description
Peer	An NTP peer or server that the device is associated with.
sent	The number of NTP packets that this device sent to the peer.
received	The number of NTP packets that this device received from the peer.

Related commands [ntp restrict](#)

show ntp status

Overview Use this command to display the status of the Network Time Protocol (NTP).

Syntax show ntp status

Mode User Exec and Privileged Exec

Example To see information about NTP status, use the command:

```
awplus# show ntp status
```

For information about the output displayed by this command, see ntp.org.

Example output from show ntp status

```
awplus#show ntp status
Reference ID      : C0A8010A (192.168.1.10)
Stratum          : 4
Ref time (UTC)   : Fri Jun 15 05:32:38 2018
System time      : 0.000002004 seconds fast of NTP time
Last offset      : -0.002578615 seconds
RMS offset       : 0.000928071 seconds
Frequency        : 5.099 ppm slow
Residual freq    : -9.120 ppm
Skew             : 17.486 ppm
Precision        : -21 (0.000000477 seconds)
Root delay       : 0.031749818 seconds
Root dispersion  : 0.133974627 seconds
Update interval  : 65.3 seconds
Leap status      : Normal
```

35

SNMP Commands

- Contents**
- **Introduction** on page 1801
 - **alias (interface)** on page 1802
 - **debug snmp** on page 1803
 - **show counter snmp-server** on page 1805
 - **show debugging snmp** on page 1810
 - **show running-config snmp** on page 1811
 - **show snmp-server** on page 1812
 - **show snmp-server community** on page 1813
 - **show snmp-server group** on page 1814
 - **show snmp-server trap** on page 1815
 - **show snmp-server user** on page 1816
 - **show snmp-server view** on page 1817
 - **snmp trap link-status** on page 1818
 - **snmp trap link-status suppress** on page 1819
 - **snmp-server** on page 1821
 - **snmp-server community** on page 1823
 - **snmp-server contact** on page 1824
 - **snmp-server enable trap** on page 1825
 - **snmp-server engineID local** on page 1829
 - **snmp-server engineID local reset** on page 1831
 - **snmp-server group** on page 1832
 - **snmp-server host** on page 1834
 - **snmp-server legacy-ifadminstatus** on page 1837
 - **snmp-server location** on page 1838
 - **snmp-server source-interface** on page 1839
 - **snmp-server startup-trap-delay** on page 1840
 - **snmp-server system-name** on page 1841
 - **snmp-server user** on page 1842
 - **snmp-server view** on page 1845
 - **snmp-server vrf** on page 1846
 - **test snmp trap snmp** on page 1847
 - **undebug snmp** on page 1848

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](#).

alias (interface)

Overview Use this command to set an alias name for a port, as returned by the SNMP ifMIB in OID 1.3.6.1.2.1.31.1.1.18.

Use the **no** variant of this command to remove an alias name from a port.

Syntax alias <ifAlias>
no alias

Parameter	Description
<ifAlias>	64 character name for an interface in a network management system. All printable characters are valid.

Default Not set.

Mode Interface Configuration

Usage notes The interface alias can also be set via SNMP.
Third-party management systems often use standard MIBs to access device information. Network managers can specify an alias interface name to provide a non-volatile way to access the interface.

Example To configure the alias interface name 'uplink_a' for eth1, use the following commands:

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

To remove an alias interface name from eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 **show debugging snmp**
commands **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 The following shows typical output.

Example output from the show counter snmp-server command

SNMP-SERVER counters	
inPkts	11
inBadVersions	0
inBadCommunityNames	0
inBadCommunityUses	0
inASNParseErrs	0
inTooBig	0
inNoSuchNames	0
inBadValues	0
inReadOnly	0
inGenErrs	0
inTotalReqVars	9
inTotalSetVars	0
inGetRequests	2
inGetNexts	9
inSetRequests	0
inGetResponses	0
inTraps	0
outPkts	11
outTooBig	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

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

Parameter	Meaning
	permitted from SNMP managers using the SNMP community named in the message.
inASNParseErrs	The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.
inTooBigs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inNoSuchNames	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inBadValues	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inReadOnlyls	The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error- status field. This indicates that there is an incorrect implementations of the SNMP.
inGenErrs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.
inTotalReqVars	The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.
inTotalSetVars	The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set- Request PDUs.
inGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.
inGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.
inSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.

Parameter	Meaning
inGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.
inTraps	The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.
outPkts	The number of SNMP Messages that the SNMP agent has sent.
outTooBigs	The number of SNMP PDUs that the SNMP agent has generated with the value 'tooBig' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outNoSuchNames	The number of SNMP PDUs that the SNMP agent has generated with the value 'noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outBadValues	The number of SNMP PDUs that the SNMP agent has generated with the value 'badValue' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGenErrs	The number of SNMP PDUs that the SNMP agent has generated with the value 'genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has generated.
outGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has generated.
outSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has generated.
outGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has generated.
outTraps	The number of SNMP Trap PDUs that the SNMP agent has generated.
UnsupportedSecLevels	The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent.
NotInTimeWindows	The number of received packets that the SNMP agent has dropped because they appeared

Parameter	Meaning
	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 [show snmp-server](#)
commands

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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

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 The following shows typical output.

Example output from the show snmp-server group command

```
SNMP group information:
Group name ..... guireadgroup
Security Level ..... priv
Read View ..... guiview
Write View ..... none
Notify View ..... none

Group name ..... guiwritegroup
Security Level ..... priv
Read View ..... none
Write View ..... guiview
Notify View ..... none
```

Related commands [show snmp-server](#)
[snmp-server group](#)

show snmp-server trap

Overview Use this command to display the status of the SNMP traps.

Syntax show snmp-server trap

Mode Privileged Exec

Example To display the SNMP traps status, use the commands:

```
awplus# show snmp-server trap
```

Output The following shows typical output.

Example output from: show snmp-server trap

```
awplus#show snmp-server trap
ATMF traps ..... Disabled
ATMF Link traps ..... Disabled
ATMF Node traps ..... Disabled
ATMF Guest Node traps ..... Enabled
ATMF Reboot Rolling traps ..... Disabled
Authentication failure ..... Disabled
BGP traps ..... Disabled
CWM Access Point traps ..... Enabled
DHCP Snooping traps ..... Disabled
EPSR traps ..... Disabled
LLDP traps ..... Disabled
Loop Protection traps ..... Disabled
MSTP traps ..... Disabled
NSM traps ..... Disabled
OSPF traps ..... Disabled
PIM traps ..... Disabled
Power-inline traps ..... Disabled
QoS Storm Protection traps ..... Enabled
RMON traps ..... Disabled
MAC address Thrash Limiting traps .... Disabled
UDLD traps ..... Disabled
VCS traps ..... Disabled
VRRP traps ..... Disabled
MRP traps ..... Enabled
Wireless traps ..... Disabled
```

Related commands [show snmp-server](#)
[snmp-server enable trap](#)

show snmp-server user

Overview This command displays the SNMP server users and is used with SNMP version 3 only.

Syntax show snmp-server user

Mode Privileged Exec

Example To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

Output The following shows typical output.

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 The following shows typical output.

Example output from the show snmp-server view command

```
SNMP view information:
View Name ..... view1
OID ..... 1
Type ..... included
```

Related commands [show snmp-server](#)
[snmp-server view](#)

snmp trap link-status

Overview Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).
Use the **no** variant of this command to disable the sending of link status notifications.

Syntax snmp trap link-status [enterprise]
no snmp trap link-status

Parameter	Description
enterprise	Send an Allied Telesis enterprise type of link trap.

Default Disabled

Mode Interface Configuration

Usage notes The link status notifications can be enabled for the following interface types:

- Ethernet (e.g. 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 eth1 use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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 eth1 after 10 notifications in 40 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To stop suppressing link status notifications for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
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**.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]

Parameter	Description
ip	Enable or disable the SNMP agent for IPv4.
ipv6	Enable or disable the SNMP agent for IPv6.

Default By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

Mode Global Configuration

Examples To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

Related commands

- show snmp-server**
- show snmp-server community**
- show snmp-server user**
- snmp-server community**
- snmp-server contact**
- snmp-server enable trap**
- snmp-server engineID local**
- snmp-server group**
- snmp-server host**
- snmp-server location**
- snmp-server view**

snmp-server community

Overview This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read-only. If the view parameter is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

Syntax `snmp-server community <community-name> [view <view-name>|ro|rw]`
`no snmp-server community <community-name>`

Parameter	Description
<community-name>	Community name. The community name is a case sensitive string of up to 20 characters.
view	Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
<view-name>	View name. The view name is a string up to 20 characters long and is case sensitive.
ro	Read-only community.
rw	Read-write community.

Default The default access mode is Read-only.

Mode Global Configuration

Example Use the following commands to create an SNMP community called 'public' with read-only access to all MIB variables from any management station:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server community public ro
```

Use the following commands to remove an SNMP community called 'public'

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server community public
```

Related commands [show snmp-server](#)
[show snmp-server community](#)
[snmp-server view](#)

snmp-server contact

Overview This command sets the contact information for the system. The contact name is:

- displayed in the output of the **show system** command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

Syntax snmp-server contact <contact-info>
no snmp-server contact

Parameter	Description
<contact-info>	The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the system contact information to "example@example.com", use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact example@example.com
```

Related commands **show system**
snmp-server location
snmp-server system-name
snmp-server group

snmp-server enable trap

Overview Use this command to enable the transmission of the specified notifications (traps) on your device.

Note that the Environmental Monitoring traps defined in the AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications.

Syntax snmp-server enable trap <trap-list>
no snmp-server enable trap <trap-list>

Depending on your device model, you can enable some or all of the traps in the following table:

Parameter	Description
atmf	AMF traps.
atmfguestnode	AMF guest node traps.
atmflink	AMF link traps.
atmfnode	AMF node traps.
atmfrr	AMF reboot-rolling traps.
auth	Authentication failure.
bgp	BGP traps.
chassis	Chassis traps.
cwmap	Access Point traps with the AWC wireless manager.
dhcpsnooping	DHCP snooping and ARP security traps. These notifications must also be set using the ip dhcp snooping violation command, and/or the arp security violation command.
epsr	EPSR traps.
g8032	G.8032 ERP traps.
lldp	Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the lldp notifications command, and/or the lldp med-notifications command.
loopprot	Loop Protection traps.
low-memory	Traps that are generated when available memory drops beneath low, very low, and critical thresholds, and when it returns to normal. The traps are: 1.3.6.1.4.1.207.8.4.4.3.7.0 memoryTraps 1.3.6.1.4.1.207.8.4.4.3.7.0.1 memoryLowTrap 1.3.6.1.4.1.207.8.4.4.3.7.0.2 memoryVeryLowTrap 1.3.6.1.4.1.207.8.4.4.3.7.0.3 memoryCriticalTrap (However, note that when the system reaches the critical memory threshold, it reboots before a trap can be sent.) 1.3.6.1.4.1.207.8.4.4.3.7.0.4 memoryReturnToNormalTrap

Parameter	Description
	1.3.6.1.4.1.207.8.4.4.3.7.0.5 vcstackId
mac-change	MAC address changed.
mac-move	MAC address moved between interface.
mac-threshold	MAC address table reaches a threshold limit.
mstp	MSTP traps.
nsm	NSM traps.
ospf	OSPF traps.
pim	PIM traps.
power-inline	Power-inline traps (Power Ethernet MIB RFC 3621).
qsp	QoS Storm Protection.
rmon	RMON traps.
thrash-limit	MAC address Thrash Limiting traps.
vcs	VCS traps. Note that to see VCS resiliency link traps, you have to use the vcs-resiliency-link parameter too, as shown below.
vcs vcs-resiliency-link	VCS resiliency link traps. You will only see these traps if you enter both vcs and vcs-resiliency-link .
vrrp	Virtual Router Redundancy (VRRP) traps.
ufo	Upstream Forwarding Only (UFO) traps.

Default Disabled

Mode Global Configuration

Usage notes This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the **snmp trap link-status** command.

To specify where notifications are sent, use the **snmp-server host** command.

Note that you can enable (or disable) multiple traps with a single command, by specifying a space-separated list of traps.

Examples To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send 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 5.5.4-2.3: **low-memory** parameter added
Version 5.5.4-0.1: **vcs vcs-resiliency-link** parameter added
Version 5.5.1-2.1: **mac-change**, **mac-move**, and **mac-threshold** parameters added
Version 5.5.1-1.1: **atmfguestnode** and **cwmap** parameters added
Version 5.4.7-2.1: **ufo** parameter added

snmp-server engineID local

Overview Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command.

Note that the **snmp-server engineID local reset** command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

Syntax snmp-server engineID local {<engine-id>|default}
no snmp-server engineID local

Parameter	Description
<engine-id>	Specify SNMPv3 Engine ID value, a string of up to 27 characters.
default	Set SNMPv3 engine ID to a system generated value by resetting the SNMPv3 engine, provided the current engine ID is user defined. If the current engine ID is system generated, use the snmp-server engineID local reset command to force the system to generate a new engine ID.

Mode Global Configuration

Usage notes All devices must have a unique engine ID which is permanently set unless it is configured by the user.

Example To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

Output The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server ..... Enabled
IP Protocol ..... IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) ..... 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server ..... Enabled
IP Protocol ..... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ..... 0x80001f888029af52e149198483
```

Related commands [show snmp-server](#)
[snmp-server engineID local reset](#)
[snmp-server group](#)

snmp-server engineID local reset

Overview Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the **snmp-server engineID local** command to set SNMPv3 engine ID to a system generated value.

Syntax snmp-server engineID local reset

Mode Global Configuration

Example To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

Related commands **snmp-server engineID local**
show snmp-server

snmp-server group

Overview This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

Syntax `snmp-server group <groupname> {auth|noauth|priv} [read <readname>|write <writename>|notify <notifysname>]`
`no snmp-server group <groupname>`

Parameter	Description
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
auth	Authentication.
noauth	No authentication and no encryption.
priv	Authentication and encryption.
read	Configure read view.
<readname>	Read view name.
write	Configure write view.
<writename>	Write view name. The view name is a string up to 20 characters long and is case sensitive.
notify	Configure notify view.
<notifysname>	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 the SNMP group called 'usergroup', use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server group usergroup
```

Related commands

- snmp-server**
- show snmp-server**
- show snmp-server group**
- show snmp-server user**

snmp-server host

Overview This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6)
- inform or trap messages
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

When VRF-lite is configured, you can apply this command to a specific VRF instance.

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>`

Syntax (VRF-Lite) `snmp-server host {<ipv4-address>|<ipv6-address>} [vrf <vrf-
name>] [informs|traps] version {1|2c|3} {auth|noauth|priv}
{<community-name>|<user-name>}`
`no snmp-server host {<ipv4-address>|<ipv6-address>} [vrf <vrf-
name>] [informs|traps] version {1|2c|3} {auth|noauth|priv}
{<community-name>|<user-name>}`

Parameter	Description
<i><ipv4-address></i>	IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.
<i><ipv6-address></i>	IPv6 trap host address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
vrf <i><vrf-name></i>	Specify the VRF instance to use. If you do not specify an instance it will use the global VRF.
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.
auth	Authentication.
noauth	No authentication.
priv	Encryption.
<i><community-name></i>	The SNMPv1 or SNMPv2c community name.
<i><user-name></i>	SNMPv3 user name.

Default No host is defined.

Mode Global Configuration

Usage notes You can test connectivity to the host by using the command **test snmp** **trap snmp**.

Examples To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name 'private', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 2001:db8::8a2e:7334 version 2c
private
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to an IPv4 host destination 192.168.1.2 with the SNMPv2c community name 'public' and on a VRF named 'red', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.1.2 vrf red version 2c
public
```

Related commands

- snmp trap link-status**
- snmp-server enable trap**
- snmp-server view**
- test snmp trap snmp**

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

snmp-server legacy-ifadminstatus

Overview Use this command to set the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state.

The **no** variant of this command sets the ifAdminStatus to reflect the administrative state of the interface.

Syntax snmp-server legacy-ifadminstatus
no snmp-server legacy-ifadminstatus

Default Legacy ifAdminStatus is turned off by default, so by default the SNMP ifAdminStatus reflects the administrative state of the interface.

Mode Global Configuration

Usage notes Note that if you enable Legacy ifAdminStatus, the ifAdminStatus will report a link's status as Down when the link has been blocked by a process such as loop protection.

Example To turn on Legacy ifAdminStatus, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server legacy-ifadminstatus
```

Related commands [show interface](#)

snmp-server location

Overview This command sets the location of the system. The location is:

- displayed in the output of the **show system** command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

Syntax snmp-server location <location-name>
no snmp-server location

Parameter	Description
<location-name>	The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

Related commands **show snmp-server**
show system
snmp-server contact
snmp-server system-name

snmp-server source-interface

Overview Use this command to specify the originating interface for SNMP traps or informs. An interface specified by this command must already have an IP address assigned to it.

Use the **no** variant of this command to reset the interface to its default value (the originating egress interface).

Syntax `snmp-server source-interface {traps|informs} <interface-name>`
`no snmp-server source-interface {traps|informs}`

Parameter	Description
traps	SNMP traps.
informs	SNMP informs.
<interface-name>	Interface name (must already have an IP address assigned).

Default The originating egress interface of the traps and informs messages

Mode Global Configuration

Usage notes When an SNMP server sends an SNMP trap or inform message, the message carries the notification IP address of its originating interface. Use this command to assign this interface.

Example The following commands set eth1 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 eth1
```

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
<i><delay-time></i>	Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds.

Default The SNMP server trap delay time is 30 seconds. The no variant restores the default.

Mode Global Configuration

Example To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

Validation Commands **show snmp-server**

snmp-server system-name

- Overview** Use this command to set the name of the system. The name is stored in the MIB object sysName.
- Note that this command does not set the hostname or change the name in the command prompt. Use the [hostname](#) command to do that.
- Use the **no** variant of this command to remove the system name.

- Syntax** snmp-server system-name <name>
no snmp-server system-name

Parameter	Description
<name>	The name of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

- Default** None

- Mode** Global Configuration

- Example** To set the system name to ExampleDevice, use the commands:
- ```
awplus# configure terminal
awplus(config)# snmp-server system-name ExampleDevice
```

- Related commands** [hostname](#)  
[show snmp-server](#)  
[snmp-server contact](#)  
[snmp-server location](#)

- Command changes** Version 5.5.5-2.1: command added

## snmp-server user

**Overview** Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

**Syntax** snmp-server user <username> <groupname> [encrypted] [auth {md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]  
no snmp-server user <username>

| Parameter          | Description                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <username>         | User name. The user name is a string up to 20 characters long and is case sensitive.                |
| <groupname>        | Group name. The group name is a string up to 20 characters long and is case sensitive.              |
| encrypted          | Use the encrypted parameter when you want to enter encrypted passwords.                             |
| auth               | Authentication protocol.                                                                            |
| md5                | MD5 Message Digest Algorithms.                                                                      |
| sha                | SHA Secure Hash Algorithm.                                                                          |
| <auth-password>    | Authentication password. The password is a string of 8 to 20 characters long and is case sensitive. |
| priv               | Privacy protocol.                                                                                   |
| des                | DES: Data Encryption Standard.                                                                      |
| aes                | AES: Advanced Encryption Standards.                                                                 |
| <privacy-password> | Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.        |

**Mode** Global Configuration

**Usage notes** Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.
- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

**Examples** To add SNMP user authuser as a member of group 'usergroup', with authentication protocol MD5, authentication password 'Authpass', privacy protocol AES and privacy password 'Privpass' use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv aes Privpass
```

Validate the user is assigned to the group using the **show snmp-server user** command:

| awplus#show snmp-server user |            |       |         |
|------------------------------|------------|-------|---------|
| Name                         | Group name | Auth  | Privacy |
| -----                        | -----      | ----- | -----   |
| authuser                     | usergroup  | md5   | aes     |

To enter existing SNMP user 'authuser' with existing passwords as a member of group 'newusergroup' with authentication protocol MD5 with the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, and privacy protocol AES with the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser newusergroup encrypted
auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv aes
0x0e0133db5453ebd03822b004eeacb6608f
```

**NOTE:** Copy and paste the encrypted passwords from the or the displayed, using the and 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><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](#)

## snmp-server vrf

**Overview** Use this command to isolate the SNMP Agent to operate within a previously configured non-global named VRF. This means the SNMP Agent can only respond to requests from SNMP Managers operating within the same VRF.

Use the **no** variant of this command to revert the SNMP Agent to operating within the default global VRF.

**Syntax** `snmp-server vrf <vrf-name>`  
`no snmp-server vrf`

| Parameter                     | Description                         |
|-------------------------------|-------------------------------------|
| <code>vrf</code>              | The VRF instance to operate within. |
| <code>&lt;vrf-name&gt;</code> | The VRF instance name.              |

**Default** Global VRF

**Mode** Global Configuration

**Examples** To configure the SNMP Agent to operate within the VRF instance named 'red', use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server vrf red
```

To revert the SNMP Agent to operating within the default global VRF, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server vrf
```

**Related commands** [show snmp-server](#)  
[snmp-server](#)

**Command changes** Version 5.5.2-2.1: command added

# test snmp trap snmp

**Overview** Use this command to test connectivity between the AlliedWare Plus device and an SNMP manager. The command tests the connectivity by sending a one-off coldStart or warmStart trap.

It does not matter whether you send a coldStart or warmStart trap; either trap lets you test the connectivity.

**Syntax** test snmp trap snmp coldstart  
test snmp trap snmp warmstart

| Parameter | Description                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------|
| coldstart | Send a one-off coldStart trap. This trap indicates that the SNMP agent is restarting with a configuration change.    |
| warmstart | Send a one-off warmStart trap. This trap indicates that the SNMP agent is restarting without a configuration change. |

**Default** n/a

**Mode** Privileged Exec

**Example** To send a one-off coldStart trap to the SNMP manager configured on the device, use the command:

```
awplus# test snmp trap snmp coldstart
```

**Related commands** [snmp-server host](#)

**Command changes** Version 5.5.4-2.3: command added

# undebug snmp

**Overview** This command applies the functionality of the no **debug snmp** command.

# 36

## LLDP Commands

- Contents**
- **Introduction** on page 1850
  - **clear lldp statistics** on page 1851
  - **clear lldp table** on page 1852
  - **debug lldp** on page 1853
  - **lldp faststart-count** on page 1855
  - **lldp holdtime-multiplier** on page 1856
  - **lldp management-address** on page 1857
  - **lldp med-notifications** on page 1859
  - **lldp med-tlv-select** on page 1860
  - **lldp non-strict-med-tlv-order-check** on page 1862
  - **lldp notification-interval** on page 1863
  - **lldp notifications** on page 1864
  - **lldp port-number-type** on page 1865
  - **lldp reinit** on page 1867
  - **lldp run** on page 1868
  - **lldp timer** on page 1869
  - **lldp tlv-select** on page 1870
  - **lldp transmit receive** on page 1872
  - **lldp tx-delay** on page 1874
  - **location civic-location configuration** on page 1875
  - **location civic-location identifier** on page 1880
  - **location coord-location configuration** on page 1881
  - **location coord-location identifier** on page 1883
  - **location elin-location** on page 1884
  - **show debugging lldp** on page 1885
  - **show lldp** on page 1887
  - **show lldp interface** on page 1890
  - **show lldp local-info** on page 1893
  - **show lldp neighbors** on page 1898
  - **show lldp neighbors detail** on page 1900
  - **show lldp statistics** on page 1904
  - **show lldp statistics interface** on page 1907
  - **show location** on page 1910

# Introduction

**Overview** LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (see the [Support for Allied Telesis Enterprise MIBs in AlliedWare Plus](#)).

For more information about LLDP, see the [LLDP Feature Overview and Configuration Guide](#).

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (see the [SNMP Feature Overview and Configuration Guide](#)).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.

# clear lldp statistics

**Overview** This command clears all LLDP statistics (packet and event counters) associated with specified ports. If no port list is supplied, LLDP statistics for all ports are cleared.

**Syntax** `clear lldp statistics [interface <port-list>]`

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <port-list> | The ports for which the statistics are to be cleared. |

**Mode** Privileged Exec

**Examples** To clear the LLDP statistics on eth1 and eth2 use the command:

```
awplus# clear lldp statistics interface eth1,eth2
```

To clear all LLDP statistics for all ports, use the command:

```
awplus# clear lldp statistics
```

**Related commands** [show lldp statistics](#)  
[show lldp statistics interface](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V  
Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

# clear lldp table

**Overview** This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

**Syntax** `clear lldp table [interface <port-list>]`

| Parameter   | Description                                                          |
|-------------|----------------------------------------------------------------------|
| <port-list> | The ports for which the neighbor information table is to be cleared. |

**Mode** Privileged Exec

**Examples** To clear the table of neighbor information received on eth1 and eth2, use the command:

```
awplus#clear lldp table interface eth1,eth2
```

To clear the entire table of neighbor information received through all ports, use the command:

```
awplus# clear lldp table
```

**Related commands** [show lldp neighbors](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V



## debug lldp

**Overview** This command enables specific LLDP debug for specified ports. When LLDP debugging is enabled, diagnostic messages are entered into the system log. If no port list is supplied, the specified debugging is enabled for all ports.

The **no** variant of this command disables specific LLDP debug for specified ports. If no port list is supplied, the specified debugging is disabled for all ports.

**Syntax** debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]  
debug lldp operation  
no debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]  
no debug lldp operation  
no debug lldp all

| Parameter   | Description                                      |
|-------------|--------------------------------------------------|
| rx          | LLDP receive debug.                              |
| rxpkt       | Raw LLDPDUs received in hex format.              |
| tx          | LLDP transmit debug.                             |
| txpkt       | Raw Tx LLDPDUs transmitted in hex format.        |
| <port-list> | The ports for which debug is to be configured.   |
| operation   | Debug for LLDP internal operation on the switch. |
| all         | Disables all LLDP debugging for all ports.       |

**Default** By default no debug is enabled for any ports.

**Mode** Privileged Exec

**Examples** To enable debugging of LLDP receive on eth1 and eth2, use the command:

```
awplus# debug lldp rx interface eth1,eth2
```

To enable debugging of LLDP transmit with packet dump on all ports, use the command:

```
awplus# debug lldp tx txpkt
```

To disable debugging of LLDP receive on eth1 and eth2, use the command:

```
awplus# no debug lldp rx interface eth1,eth2
```

To turn off all LLDP debugging on all ports, use the command:

```
awplus# no debug lldp all
```

**Related commands** [show debugging lldp](#)  
[show running-config lldp](#)  
[terminal monitor](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## lldp faststart-count

**Overview** Use this command to configure the fast start count for LLDP-MED. The fast start count determines the number of fast start advertisements a port sends when initiating LLDP-MED advertisements. This occurs, for example, when a new LLDP-MED capable device is detected.

The **no** variant of this command resets the LLDP-MED fast start count to the default (3).

**Syntax** `lldp faststart-count <1-10>`  
`no lldp faststart-count`

| Parameter | Description                                      |
|-----------|--------------------------------------------------|
| <1-10>    | The number of fast start advertisements to send. |

**Default** The default fast start count is 3.

**Mode** Global Configuration

**Examples** To set the fast start count to 5, use the command:

```
awplus# configure terminal
awplus(config)# lldp faststart-count 5
```

To reset the fast start count to the default setting (3), use the command:

```
awplus# configure terminal
awplus(config)# no lldp faststart-count
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## lldp holdtime-multiplier

**Overview** This command sets the holdtime multiplier value. This value is multiplied by the transmit interval to determine the advertised Time To Live (TTL) value advertised to neighbors.

The **no** variant of this command sets the multiplier back to its default.

**Syntax** `lldp holdtime-multiplier <2-10>`  
`no lldp holdtime-multiplier`

| Parameter                 | Description            |
|---------------------------|------------------------|
| <code>&lt;2-10&gt;</code> | The multiplier factor. |

**Default** The default holdtime multiplier value is 4.

**Mode** Global Configuration

**Usage** The Time-To-Live (TTL) specifies how long the advertised information remains valid for neighbors. If the TTL expires before receiving an update, the neighbor removes the information from its database.

**Examples** To set the holdtime multiplier to 2, use the commands:

```
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 2
```

To set the holdtime multiplier back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp holdtime-multiplier 2
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp management-address

**Overview** This command sets the IPv4 address to be advertised to neighbors (in the Management Address TLV) via the specified ports. This address will override the default address for these ports.

The **no** variant of this command clears the user-configured management IP address advertised to neighbors via the specified ports. The advertised address reverts to the default.

**Syntax** `lldp management-address <ipaddr>`  
`no lldp management-address`

| Parameter                   | Description                                                                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipaddr&gt;</code> | The IPv4 address to be advertised to neighbors, in dotted decimal format. This must be one of the IP addresses already configured on the device. |

**Default** The local loopback interface's primary IPv4 address, if configured. Alternatively, if no IP addresses are configured, the MAC address of the device's baseboard.

**Mode** Interface Configuration

**Usage notes** To see the management address that will be advertised, use the [show lldp interface](#) command or [show lldp local-info](#) command.

**Examples** To set the management address advertised by eth1 and eth2 to 192.168.1.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by eth1 and eth2, and revert to using the default address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp management-address
```

**Related commands** [show lldp interface](#)  
[show lldp local-info](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V  
Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

# lldp med-notifications

**Overview** Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the **no** variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

**Syntax** `lldp med-notifications`  
`no lldp med-notifications`

**Default** The sending of LLDP-MED notifications is disabled by default.

**Mode** Interface Configuration

**Examples** To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp med-notifications
```

To disable the sending of LLDP-MED notifications relating to eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp med-notifications
```

**Related commands** [lldp notification-interval](#)  
[lldp notifications](#)  
[snmp-server enable trap](#)  
[show lldp interface](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V  
Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

## lldp med-tlv-select

**Overview** Use this command to enable LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via the specified ports. The LLDP-MED Capabilities TLV must be enabled before any of the other LLDP-MED Organizationally Specific TLVs are enabled.

Use the **no** variant of this command to disable the specified LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via these ports. In order to disable the LLDP-MED Capabilities TLV, you must also disable the rest of these TLVs. Disabling all these TLVs disables LLDP-MED advertisements.

**Syntax** `lldp med-tlv-select [capabilities] [inventory-management]`  
`lldp med-tlv-select all`  
`no lldp med-tlv-select [capabilities] [location] [inventory-management]`  
`no lldp med-tlv-select all`

| Parameter            | Description                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| capabilities         | LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV from IEEE 802.3 Organizationally Specific TLVs is also automatically included in LLDP-MED advertisements, whether or not it has been explicitly enabled by the <b>lldp tlv-select</b> command. |
| inventory-management | Inventory Management TLV Set, including the following TLVs: <ul style="list-style-type: none"><li>• Hardware Revision</li><li>• Firmware Revision</li><li>• Software Revision</li><li>• Serial Number</li><li>• Manufacturer Name</li><li>• Model Name</li><li>• Asset ID</li></ul>  |
| all                  | All LLDP-MED Organizationally Specific TLVs.                                                                                                                                                                                                                                         |

**Default** By default, LLDP-MED Capabilities, Network Policy, Location Identification, and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the **lldp run** command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

**Mode** Interface Configuration



**Usage notes** LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the **show lldp neighbors** command.

**Examples** To enable inclusion of the Inventory TLV Set in advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via eth1 and eth2, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp med-tlv-select all
```

**Related commands**

- lldp tlv-select**
- location civic-location identifier**
- location civic-location configuration**
- location coord-location identifier**
- location coord-location configuration**
- location elin-location**
- show lldp interface**

**Command changes**

- Version 5.5.3-1.1: Command added to AR1050V
- Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

# lldp non-strict-med-tlv-order-check

**Overview** Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the **no** variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

**Syntax** `lldp non-strict-med-tlv-order-check`  
`no lldp non-strict-med-tlv-order-check`

**Default** By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

**Mode** Global Configuration

**Usage notes** The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

**Examples** To enable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp notification-interval

**Overview** This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).  
  
The **no** variant of this command sets the notification interval back to its default.

**Syntax** `lldp notification-interval <5-3600>`  
`no lldp notification-interval`

| Parameter                   | Description              |
|-----------------------------|--------------------------|
| <code>&lt;5-3600&gt;</code> | The interval in seconds. |

**Default** The default notification interval is 5 seconds.

**Mode** Global Configuration

**Examples** To set the notification interval to 20 seconds, use the commands:  
`awplus# configure terminal`  
`awplus(config)# lldp notification-interval 20`  
To set the notification interval back to its default, use the commands:  
`awplus# configure terminal`  
`awplus(config)# no lldp notification-interval`

**Related commands** [lldp notifications](#)  
[show lldp](#)

# lldp notifications

**Overview** This command enables the sending of LLDP SNMP notifications (traps) relating to specified ports.

The **no** variant of this command disables the sending of LLDP SNMP notifications for specified ports.

**Syntax** `lldp notifications`  
`no lldp notifications`

**Default** The sending of LLDP SNMP notifications is disabled by default.

**Mode** Interface Configuration

**Examples** To enable sending of LLDP SNMP notifications for eth1 and eth2, use the commands:

```
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp notifications
```

To disable sending of LLDP SNMP notifications for eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp notifications
```

**Related commands** [lldp notification-interval](#)  
[show lldp interface](#)  
[snmp-server enable trap](#)

## lldp port-number-type

**Overview** This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. The LLDP MIB (IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions.) requires the port number value to count LLDP local port entries.

This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.

The **no** variant of this command resets the type of port identifier back to the default setting (number).

**Syntax** `lldp port-number-type [number|ifindex]`  
`no lldp port-number-type`

| Parameter | Description                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------|
| number    | Set the type of port identifier to a port number to enumerate the LLDP MIB local port entries.      |
| ifindex   | Set the type of port identifier to an interface index to enumerate the LLDP MIB local port entries. |

**Default** The default port identifier type is number. The no variant of this command sets the port identifier type to the default.

**Mode** Global Configuration

**Examples** To set the type of port identifier used to enumerate LLDP MIB local port entries to port numbers, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type number
```

To set the type of port identifier used to enumerate LLDP MIB local port entries to interface indexes, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type ifindex
```

To reset the type of port identifier used to enumerate LLDP MIB local port entries the default (port numbers), use the commands:

```
awplus# configure terminal
awplus(config)# no lldp port-number-type
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp reinit

**Overview** This command sets the value of the reinitialization delay. This is the minimum time after disabling LLDP on a port before it can reinitialize.

The **no** variant of this command sets the reinitialization delay back to its default setting.

**Syntax** `lldp reinit <1-10>`  
`no lldp reinit`

| Parameter | Description           |
|-----------|-----------------------|
| <1-10>    | The delay in seconds. |

**Default** The default reinitialization delay is 2 seconds.

**Mode** Global Configuration

**Examples** To set the reinitialization delay to 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp reinit 3
```

To set the reinitialization delay back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp reinit
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp run

**Overview** This command enables the operation of LLDP on the device.

The **no** variant of this command disables the operation of LLDP on the device. The LLDP configuration remains unchanged.

**Syntax** lldp run  
no lldp run

**Default** LLDP is disabled by default.

**Mode** Global Configuration

**Examples** To enable LLDP operation, use the commands:

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

To disable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp run
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V



# lldp timer

**Overview** This command sets the value of the transmit interval. This is the interval between regular transmissions of LLDP advertisements.

The **no** variant of this command sets the transmit interval back to its default.

**Syntax** `lldp timer <5-32768>`  
`no lldp timer`

| Parameter                    | Description                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;5-32768&gt;</code> | The transmit interval in seconds. The transmit interval must be at least four times the transmission delay timer ( <b>lldp tx-delay</b> command). |

**Default** The default transmit interval is 30 seconds.

**Mode** Global Configuration

**Examples** To set the transmit interval to 90 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp timer 90
```

To set the transmit interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp timer
```

**Related commands** **lldp tx-delay**  
**show lldp**

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp tlv-select

**Overview** This command enables one or more optional TLVs, or all TLVs, for transmission in LLDP advertisements via the specified ports. The TLVs can be specified in any order; they are placed in LLDP frames in a fixed order (as described in IEEE 802.1AB). The mandatory TLVs (Chassis ID, Port ID, Time To Live, End of LLDPDU) are always included in LLDP advertisements.

In LLDP-MED advertisements the MAC/PHY Configuration/Status TLV will be always be included regardless of whether it is selected by this command.

The **no** variant of this command disables the specified optional TLVs, or all optional TLVs, for transmission in LLDP advertisements via the specified ports.

**Syntax** `lldp tlv-select {[<tlv>]...}`  
`lldp tlv-select all`  
`no lldp tlv-select {[<tlv>]...}`  
`no lldp tlv-select all`

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <tlv>     | The TLV to transmit in LLDP advertisements. One of these keywords: <ul style="list-style-type: none"><li>• port-description (specified by the <b>description (interface)</b>)</li><li>• system-name (specified by the <b>hostname</b>)</li><li>• system-description</li><li>• system-capabilities</li><li>• management-address</li><li>• port-vlan</li><li>• port-and-protocol-vlans</li><li>• vlan-names</li><li>• protocol-ids</li><li>• mac-phy-config</li><li>• power-management (Power Via MDI TLV)</li><li>• link-aggregation</li><li>• max-frame-size</li></ul> |
| all       | All TLVs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Default** By default, no optional TLVs are included in LLDP advertisements. The MAC/PHY Configuration/Status TLV (**mac-phy-config**) is included in LLDP-MED advertisements whether or not it is selected by this command.

**Mode** Interface Configuration

**Examples** To include the management-address and system-name TLVs in advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp tlv-select management-address system-name
```

To include all optional TLVs in advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp tlv-select all
```

To exclude the management-address and system-name TLVs from advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp tlv-select management-address system-name
```

To exclude all optional TLVs from advertisements transmitted via eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp tlv-select all
```

**Related commands**

- [description \(interface\)](#)
- [hostname](#)
- [lldp med-tlv-select](#)
- [show lldp interface](#)
- [show lldp local-info](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# lldp transmit receive

**Overview** This command enables transmission and/or reception of LLDP advertisements to or from neighbors through the specified ports.

The **no** variant of this command disables transmission and/or reception of LLDP advertisements through specified ports.

**Syntax** `lldp {[transmit] [receive]}`  
`no lldp {[transmit] [receive]}`

| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| transmit  | Enable or disable transmission of LLDP advertisements via this port or ports. |
| receive   | Enable or disable reception of LLDP advertisements via this port or ports.    |

**Default** LLDP advertisement transmission and reception are enabled on all ports by default.

**Mode** Interface Configuration

**Examples** To enable transmission of LLDP advertisements on eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# no lldp transmit receive
```

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V  
Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

## lldp tx-delay

**Overview** This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

**Syntax** `lldp tx-delay <1-8192>`  
`no lldp tx-delay`

| Parameter | Description                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-8192>  | The transmission delay in seconds. The transmission delay cannot be greater than a quarter of the transmit interval ( <b>lldp timer</b> command). |

**Default** The default transmission delay timer is 2 seconds.

**Mode** Global Configuration

**Examples** To set the transmission delay timer to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

**Related commands** [lldp timer](#)  
[show lldp](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# location civic-location configuration

**Overview** Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the **no** variants of this command to delete civic address parameters from the location.

**Syntax** country <country>  
state <state>  
no state  
county <county>  
no county  
city <city>  
no city  
division <division>  
no division  
neighborhood <neighborhood>  
no neighborhood  
street-group <street-group>  
no street-group  
leading-street-direction <leading-street-direction>  
no leading-street-direction  
trailing-street-suffix <trailing-street-suffix>  
no trailing-street-suffix  
street-suffix <street-suffix>  
no street-suffix  
house-number <house-number>  
no house-number  
house-number-suffix <house-number-suffix>  
no house-number-suffix  
landmark <landmark>  
no landmark  
additional-information <additional-information>  
no additional-information

**Syntax** name <name>  
**(cont.)** no name  
postalcode <postalcode>  
no postalcode  
building <building>  
no building  
unit <unit>  
no unit  
floor <floor>  
no floor  
room <room>  
no room  
place-type <place-type>  
no place-type  
postal-community-name <postal-community-name>  
no postal-community-name  
post-office-box <post-office-box>  
no post-office-box  
additional-code <additional-code>  
no additional-code  
seat <seat>  
no seat  
primary-road-name <primary-road-name>  
no primary-road-name  
road-section <road-section>  
no road-section  
branch-road-name <branch-road-name>  
no branch-road-name  
sub-branch-road-name <sub-branch-road-name>  
no sub-branch-road-name  
street-name-pre-modifier <street-name-pre-modifier>  
no street-name-pre-modifier  
streetname-post-modifier <streetname-post-modifier>  
no streetname-post-modifier

| Parameter | Description                                                                       |
|-----------|-----------------------------------------------------------------------------------|
| <country> | Upper-case two-letter country code, as specified in ISO 3166.                     |
| <state>   | State (Civic Address (CA) Type 1): national subdivisions (state, canton, region). |



| Parameter                                     | Description                                                                        |
|-----------------------------------------------|------------------------------------------------------------------------------------|
| <code>&lt;county&gt;</code>                   | County (CA Type 2): County, parish, gun (JP), district (IN).                       |
| <code>&lt;city&gt;</code>                     | City (CA Type 3): city, township, shi (JP).                                        |
| <code>&lt;division&gt;</code>                 | City division (CA Type 4): City division, borough, city district, ward, chou (JP). |
| <code>&lt;neighborhood&gt;</code>             | Neighborhood (CA Type 5): neighborhood, block.                                     |
| <code>&lt;street-group&gt;</code>             | Street group (CA Type 6): group of streets below the neighborhood level.           |
| <code>&lt;leading-street-direction&gt;</code> | Leading street direction (CA Type 16).                                             |
| <code>&lt;trailing-street-suffix&gt;</code>   | Trailing street suffix (CA Type 17).                                               |
| <code>&lt;street-suffix&gt;</code>            | Street suffix (CA Type 18): street suffix or type.                                 |
| <code>&lt;house-number&gt;</code>             | House number (CA Type 19).                                                         |
| <code>&lt;house-number-suffix&gt;</code>      | House number suffix (CA Type 20).                                                  |
| <code>&lt;landmark&gt;</code>                 | Landmark or vanity address (CA Type 21).                                           |
| <code>&lt;additional-information&gt;</code>   | Additional location information (CA Type 22).                                      |
| <code>&lt;name&gt;</code>                     | Name (CA Type 23): residence and office occupant.                                  |
| <code>&lt;postal-code&gt;</code>              | Postal/zip code (CA Type 24).                                                      |
| <code>&lt;building&gt;</code>                 | Building (CA Type 25): structure.                                                  |
| <code>&lt;unit&gt;</code>                     | Unit (CA Type 26): apartment, suite.                                               |
| <code>&lt;floor&gt;</code>                    | Floor (CA Type 27).                                                                |
| <code>&lt;room&gt;</code>                     | Room (CA Type 28).                                                                 |
| <code>&lt;place-type&gt;</code>               | Type of place (CA Type 29).                                                        |
| <code>&lt;postal-community-name&gt;</code>    | Postal community name (CA Type 30).                                                |
| <code>&lt;post-office-box&gt;</code>          | Post office box (P.O. Box) (CA Type 31).                                           |
| <code>&lt;additional-code&gt;</code>          | Additional code (CA Type 32).                                                      |

| Parameter                                      | Description                                           |
|------------------------------------------------|-------------------------------------------------------|
| <code>&lt;seat&gt;</code>                      | Seat (CA Type 33): seat (desk, cubicle, workstation). |
| <code>&lt;primary-road-name&gt;</code>         | Primary road name (CA Type 34).                       |
| <code>&lt;road-section&gt;</code>              | Road section (CA Type 35).                            |
| <code>&lt;branch-road-name&gt;</code>          | Branch road name (CA Type 36).                        |
| <code>&lt;sub-branch-road-name&gt;</code>      | Sub-branch road name (CA Type 37).                    |
| <code>&lt;street-name-pre-modifier&gt;</code>  | Street name pre-modifier (CA Type 38).                |
| <code>&lt;street-name-post-modifier&gt;</code> | Street name post-modifier (CA Type 39).               |

**Default** By default no civic address location information is configured.

**Mode** Civic Address Location Configuration

**Usage notes** The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in ISO 3166. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see the **LLDP Feature Overview and Configuration Guide**.

To specify the civic address location, use the **location civic-location identifier** command. To delete the civic address location, use the **no** variant of the **location civic-location identifier** command.

**Examples** To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

**Related commands** **location civic-location identifier**  
**show lldp local-info**  
**show location**

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# location civic-location identifier

**Overview** Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

**Syntax** location civic-location identifier *<civic-loc-id>*  
no location civic-location identifier *<civic-loc-id>*

| Parameter                   | Description                                                 |
|-----------------------------|-------------------------------------------------------------|
| <i>&lt;civic-loc-id&gt;</i> | A unique civic address location ID, in the range 1 to 4095. |

**Default** By default there are no civic address locations.

**Mode** Global Configuration

**Usage notes** To configure the location information for this civic address location identifier, use the **location civic-location configuration** command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

**Examples** To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

**Related commands** **location civic-location configuration**  
**show location**  
**show running-config** lldp

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# location coord-location configuration

**Overview** Use this command to configure a coordinate-based location. All parameters must be configured before assigning this location identifier to a port.

**Syntax** latitude <latitude>  
lat-resolution <lat-resolution>  
longitude <longitude>  
long-resolution <long-resolution>  
altitude <altitude> {meters|floor}  
alt-resolution <alt-resolution>  
datum {wgs84|nad83-navd|nad83-mlw}

| Parameter         | Description                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <lat-resolution>  | Latitude resolution, as a number of valid bits, in the range 0 to 34.                                                             |
| <latitude>        | Latitude value in degrees in the range -90.0 to 90.0                                                                              |
| <long-resolution> | Longitude resolution, as a number of valid bits, in the range 0 to 34.                                                            |
| <longitude>       | Longitude value in degrees, in the range -180.0 to 180.0.                                                                         |
| <alt-resolution>  | Altitude resolution, as a number of valid bits, in the range 0 to 30. A resolution of 0 can be used to indicate an unknown value. |
| <altitude>        | Altitude value, in meters or floors.                                                                                              |
| meters            | The altitude value is in meters.                                                                                                  |
| floors            | The altitude value is in floors.                                                                                                  |
| datum             | The geodetic system (or datum) that the specified coordinate values are based on.                                                 |
| wgs84             | World Geodetic System 1984.                                                                                                       |
| nad83-navd        | North American Datum 1983 - North American Vertical Datum.                                                                        |
| nad83-mlw         | North American Datum 1983 - Mean Lower Low Water vertical datum.                                                                  |

**Default** By default no coordinate location information is configured.

**Mode** Coordinate Configuration

**Usage** Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise altitude is stored as a 30-bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be represented exactly—the stored binary number is converted to a decimal number for display in the output of the **show location** command. For example, a user-entered latitude value of “2.77” degrees is displayed as “2.7699999809265136718750000”.

The **lat-resolution**, **long-resolution**, and **alt-resolution** parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the **location coord-location identifier** command. To remove coordinate information, delete the coordinate location by using the **no** variant of that command.

**Example** To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# lat-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# long-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

**Related commands** **location coord-location identifier**  
**show lldp local-info**  
**show location**

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# location coord-location identifier

**Overview** Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

**Syntax** location coord-location identifier *<coord-loc-id>*  
no location coord-location identifier *<coord-loc-id>*

| Parameter                   | Description                                                      |
|-----------------------------|------------------------------------------------------------------|
| <i>&lt;coord-loc-id&gt;</i> | A unique coordinate location identifier, in the range 1 to 4095. |

**Default** By default there are no coordinate locations.

**Mode** Global Configuration

**Usage** Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To configure this coordinate location, use the **location coord-location configuration** command.

**Examples** To enter Coordinate Location Configuration mode to configure the coordinate location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)#
```

To delete coordinate location 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location coord-location identifier 1
```

**Related commands** **location coord-location configuration**  
**show lldp local-info**  
**show location**

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# location elin-location

**Overview** Use this command to create or modify an ELIN location.

Use the **no** variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

**Syntax** location elin-location <elin> identifier <elin-loc-id>  
no location elin-location identifier <elin-loc-id>

| Parameter     | Description                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <elin>        | Emergency Location Identification Number (ELIN) for Emergency Call Service (ECS), in the range 10 to 25 digits long. In North America, ELINs are typically 10 digits long. |
| <elin-loc-id> | A unique ELIN location identifier, in the range 1 to 4095.                                                                                                                 |

**Default** By default there are no ELIN location identifiers.

**Mode** Global Configuration

**Usage** Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

**Examples** To create a new ELIN location with ID 1, and configure it with ELIN "1234567890", use the commands:

```
awplus# configure terminal
awplus(config)# location elin-location 1234567890 identifier 1
```

To delete existing ELIN location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location elin-location identifier 1
```

**Related commands** [show lldp local-info](#)  
[show location](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V



## show debugging lldp

**Overview** This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

**Syntax** show debugging lldp [interface <port-list>]

| Parameter   | Description                                            |
|-------------|--------------------------------------------------------|
| <port-list> | The ports for which the LLDP debug settings are shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP debug settings for all ports, use the command:

```
awplus# show debugging lldp
```

To display LLDP debug settings for eth1 to eth2, use the command:

```
awplus# show debugging lldp interface eth1-eth2
```

**Output** The following shows typical output.

### Example output from the show debugging lldp command

|                                                                     |     |       |    |       |
|---------------------------------------------------------------------|-----|-------|----|-------|
| LLDP Debug settings:<br>Debugging for LLDP internal operation is on |     |       |    |       |
| Port                                                                | Rx  | RxPkt | Tx | TxPkt |
| -----                                                               |     |       |    |       |
| eth1                                                                | Yes | Yes   | No | No    |
| eth2                                                                | Yes | No    | No | No    |

### Parameters in the output of the show debugging lldp command

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| Port      | Port name.                                                             |
| Rx        | Whether debugging of LLDP receive is enabled on the port.              |
| RxPkt     | Whether debugging of LLDP receive packet dump is enabled on the port.  |
| Rx        | Whether debugging of LLDP transmit is enabled on the port.             |
| RxPkt     | Whether debugging of LLDP transmit packet dump is enabled on the port. |

**Related commands** [debug lldp](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# show lldp

**Overview** This command displays LLDP status and global configuration settings.

**Syntax** show lldp

**Mode** User Exec and Privileged Exec

**Example** To display LLDP status and global configuration settings, use the command:

```
awplus# show lldp
```

**Output** The following shows typical output.

**Example output from the show lldp command**

```
awplus# show lldp

LLDP Global Configuration: [Default Values]
LLDP Status Enabled [Disabled]
Notification Interval 5 secs [5]
Tx Timer Interval 30 secs [30]
Hold-time Multiplier 4 [4]
(Computed TTL value 120 secs)
Reinitialization Delay 2 secs [2]
Tx Delay 2 secs [2]

Port Number Type..... Ifindex [Port-Number]
Fast Start Count 5 [3]

LLDP Global Status:
Total Neighbor Count 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

**Parameters in the output of the show lldp command**

| Parameter                    | Description                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LLDP Status                  | Whether LLDP is enabled. Default is disabled.                                                                                                                 |
| Notification Interval        | Minimum interval between LLDP notifications.                                                                                                                  |
| Tx Timer Interval            | Transmit interval between regular transmissions of LLDP advertisements.                                                                                       |
| Hold-time Multiplier         | The holdtime multiplier. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors. |
| Reinitialization Delay       | The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.                                |
| Tx Delay                     | The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information.                      |
| Port Number Type             | The type of port identifier used to enumerate LLDP MIB local port entries, as set by the lldp port-number-type command.                                       |
| Fast Start Count             | The number of times fast start advertisements are sent for LLDP-MED.                                                                                          |
| Total Neighbor Count         | Number of LLDP neighbors discovered on all ports.                                                                                                             |
| Neighbors table last updated | The time since the LLDP neighbor table was last updated.                                                                                                      |

**Related** **show lldp interface**  
**commands** **show running-config** lldp

**Command** Version 5.5.3-1.1: Command added to AR1050V  
**changes**

# show lldp interface

**Overview** This command displays LLDP configuration settings for specified ports. If no port list is specified, LLDP configuration for all ports is displayed.

**Syntax** show lldp interface [*<port-list>*]

| Parameter                | Description                                                          |
|--------------------------|----------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports for which the LLDP configuration settings are to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP configuration settings for eth1 to eth2, use the command:

```
awplus# show lldp interface eth1-eth2
```

To display LLDP configuration settings for all ports, use the command:

```
awplus# show lldp interface
```

**Output** The following shows typical output.

### Example output from the show lldp interface command

```

awplus# show lldp interface eth1-eth2
LLDP Port Status and Configuration:

* = LLDP is inactive on this port because it is a mirror analyser port
Notification Abbreviations:
 RC = LLDP Remote Tables Change TC = LLDP-MED Topology Change
TLV Abbreviations:
 Base: Pd = Port Description Sn = System Name
 Sd = System Description Sc = System Capabilities
 Ma = Management Address
 802.1: Pv = Port VLAN ID Pp = Port And Protocol VLAN ID
 Vn = VLAN Name Pi = Protocol Identity
 802.3: Mp = MAC/PHY Config/Status Po = Power Via MDI (PoE)
 La = Link Aggregation Mf = Maximum Frame Size
 MED: Mc = LLDP-MED Capabilities Np = Network Policy
 Lo = Location Identification Pe = Extended PoE In = Inventory

```

| Port  | Rx/Tx | Notif | Management Addr | Optional TLVs Enabled for Tx |       |       |            |
|-------|-------|-------|-----------------|------------------------------|-------|-------|------------|
|       |       |       |                 | Base                         | 802.1 | 802.3 | MED        |
| eth1  | Rx Tx | RC -- | 192.168.100.123 | PdSnSdScMa                   | ----- | ----- | McNpLoPe-- |
| *eth2 | -- Tx | RC -- | 192.168.100.123 | PdSnSdScMa                   | ----- | ----- | McNpLoPe-- |

### Parameters in the output of the show lldp interface command

| Parameter                 | Description                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                      | Port name.                                                                                                                                                                                                                                               |
| Rx                        | Whether reception of LLDP advertisements is enabled on the port.                                                                                                                                                                                         |
| Tx                        | Whether transmission of LLDP advertisements is enabled on the port.                                                                                                                                                                                      |
| Notif                     | Whether sending SNMP notification for LLDP is enabled on the port: <ul style="list-style-type: none"> <li>RM = Remote Tables Change Notification</li> <li>TP = LLDP-MED Topology Change Notification</li> </ul>                                          |
| Management Addr           | Management address advertised to neighbors.                                                                                                                                                                                                              |
| Base TLVs Enabled for Tx  | List of optional Base TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Pd = Port Description</li> <li>Sn =System Name</li> <li>Sd = System Description</li> <li>Sc =System Capabilities</li> <li>Ma = Management Address</li> </ul> |
| 802.1 TLVs Enabled for Tx | List of optional 802.1 TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Pv = Port VLAN ID</li> <li>Pp = Port And Protocol VLAN ID</li> <li>Vn = VLAN Name</li> </ul>                                                                |

| Parameter                 | Description                                                                                                                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | <ul style="list-style-type: none"><li>• Pi =Protocol Identity</li></ul>                                                                                                                                                                                                 |
| 802.3 TLVs Enabled for Tx | List of optional 802.3 TLVs enabled for transmission: <ul style="list-style-type: none"><li>• Mp = MAC/PHY Configuration/Status</li><li>• Po = Power Via MDI (PoE)</li><li>• La = Link Aggregation</li><li>• Mf = Maximum Frame Size</li></ul>                          |
| MED TLVs Enabled for Tx   | List of optional LLDP-MED TLVs enabled for transmission: <ul style="list-style-type: none"><li>• Mc = LLDP-MED Capabilities</li><li>• Np = Network Policy</li><li>• Lo = Location Information,</li><li>• Pe = Extended Power-Via-MDI</li><li>• In = Inventory</li></ul> |

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

**Command changes** Version 5.5.3-1.1: Command added to AR1050V



## show lldp local-info

**Overview** This command displays local LLDP information that can be transmitted through specified ports. If no port list is entered, local LLDP information for all ports is displayed.

**Syntax** `show lldp local-info [base] [dot1] [dot3] [med] [interface <port-list>]`

| Parameter   | Description                                               |
|-------------|-----------------------------------------------------------|
| base        | Information for base TLVs.                                |
| dot1        | Information for 802.1 TLVs.                               |
| dot3        | Information for 802.3 TLVs.                               |
| med         | Information for LLDP-MED TLVs.                            |
| <port-list> | The ports for which the local information is to be shown. |

**Mode** User Exec and Privileged Exec

**Usage notes** Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements (**lldp transmit receive** command)
- which TLVs it is configured to send (**lldp tlv-select** command, **lldp med-tlv-select** command)

**Examples** To display local information transmitted via eth1, use the command:

```
awplus# show lldp local-info interface eth1
```

To display local information transmitted via all ports, use the command:

```
awplus# show lldp local-info
```

**Output** The following shows typical output.

**Example output from show lldp local-info**

```
LLDP Local Information:

Local eth1: Chassis ID Type MAC address
Chassis ID 1234.0000.0000
Port ID Type Interface name
Port ID eth1
TTL 120
Port Description eth1

System Name awplus
System Description Allied Telesis router/switch, Software
 (AlliedWare Plus) Version 5.5.4-2.3

System Capabilities - Supported .. Router
 - Enabled Router

Management Address 1234.0000.0000
Port VLAN ID (PVID) 1
Port & Protocol VLAN - Supported . No
 - Enabled ... No
 - VIDs 0

Port & Protocol VLAN - Supported . No
 - Enabled ... No
 - VIDs 0

Protocol IDs 0800, 0806, 86dd
MAC/PHY Auto-negotiation Supported, Disabled
 Advertised Capability [none]
 Operational MAU Type Unknown (0)
Power Via MDI (PoE) [not supported]
 Port Class PD
 Pair Control Ability Disabled
 Power Source Unknown Type 0

Link Aggregation Supported, Disabled
Maximum Frame Size 1500
LLDP-MED Device Type Network Connectivity
LLDP-MED Capabilities LLDP-MED Capabilities, Network Policy,
 Location Identification,
 Extended Power - PD, Inventory

Network Policy [not configured]
Location Identification [not configured]

Extended Power Via MDI (PoE) PD
 Power Source Unknown Type 0
 Power Priority Unknown
 Power Value 18.8 Watts

Inventory Management:
 Hardware Revision -
 Firmware Revision -
 Software Revision 5.5.4-2.3
 Serial Number A10454RD9853ADE0
 Manufacturer Name Allied Telesis Inc.
 Model Name AT-TQxxxxx
 Asset ID [zero length]
```

### Parameters in the output of show lldp local-info

| Parameter                        | Description                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Chassis ID Type                  | Type of the Chassis ID.                                                                                            |
| Chassis ID                       | Chassis ID that uniquely identifies the local device.                                                              |
| Port ID Type                     | Type of the Port ID.                                                                                               |
| Port ID                          | Port ID of the local port through which advertisements are sent.                                                   |
| TTL                              | Number of seconds that the information advertised by the local port remains valid.                                 |
| Port Description                 | Port description of the local port, as specified by the <b>description (interface)</b> .                           |
| System Name                      | System name, as specified by the <b>hostname</b> .                                                                 |
| System Description               | System description.                                                                                                |
| System Capabilities (Supported)  | Capabilities that the local port supports.                                                                         |
| System Capabilities (Enabled)    | Enabled capabilities on the local port.                                                                            |
| Management Addresses             | Management address associated with the local port. To change this, use the <b>lldp management-address</b> command. |
| Port VLAN ID (PVID)              | VLAN identifier associated with untagged or priority tagged frames received via the local port.                    |
| Port & Protocol VLAN (Supported) | Whether Port & Protocol VLANs (PPV) is supported on the local port.                                                |
| Port & Protocol VLAN (Enabled)   | Whether the port is in one or more Port & Protocol VLANs.                                                          |
| Port & Protocol VLAN (VIDs)      | List of identifiers for Port & Protocol VLANs that the port is in.                                                 |
| VLAN Names                       | List of VLAN names for VLANs that the local port is assigned to.                                                   |
| Protocol IDs                     | List of protocols that are accessible through the local port.                                                      |
| MAC/PHY Auto-negotiation         | Auto-negotiation support and current status of the 802.3 LAN on the local port.                                    |

| Parameter                    | Description                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Power Via MDI (PoE)          | PoE-capability and current status on the local port.                                                            |
| Port Class                   | Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device).                                   |
| Pair Control Ability         | Whether power pair selection can be controlled.                                                                 |
| Power Pairs                  | Which power pairs are selected for power ("Signal Pairs" or "Spare Pairs") if pair selection can be controlled. |
| Power Class                  | The power class of the PD device on the port (class 0, 1, 2, 3 or 4).                                           |
| Link Aggregation             | Whether the link is capable of being aggregated and it is currently in an aggregation.                          |
| Aggregated Port-ID           | Aggregated port identifier.                                                                                     |
| Maximum Frame Size           | The maximum frame size capability of the implemented MAC and PHY.                                               |
| LLDP-MED Device Type         | LLDP-MED device type.                                                                                           |
| LLDP-MED Capabilities        | Capabilities LLDP-MED capabilities supported on the local port.                                                 |
| Network Policy               | List of network policies configured on the local port.                                                          |
| VLAN ID                      | VLAN identifier for the port for the specified application type.                                                |
| Tagged Flag                  | Whether the VLAN ID is to be used as tagged or untagged.                                                        |
| Layer-2 Priority:            | Layer 2 User Priority (in the range 0 to 7).                                                                    |
| DSCP Value                   | Diffserv codepoint (in the range 0 to 63).                                                                      |
| Location Identification      | Location configured on the local port.                                                                          |
| Extended Power Via MDI (PoE) | PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.       |
| Power Source                 | The power source the switch currently uses; either primary power or backup power.                               |

| Parameter            | Description                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power Priority       | The power priority configured on the port; either critical, high or low.                                                                                 |
| Power Value          | The total power the switch can source over a maximum length cable to a PD device on the port. The value shows the power value in Watts from the PD side. |
| Inventory Management | Inventory information for the device.                                                                                                                    |

**Related commands** [description \(interface\)](#)  
[hostname](#)  
[lldp transmit receive](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## show lldp neighbors

**Overview** This command displays a summary of information received from neighbors via specified ports. If no port list is supplied, neighbor information for all ports is displayed.

**Syntax** `show lldp neighbors [interface <port-list>]`

| Parameter   | Description                                                  |
|-------------|--------------------------------------------------------------|
| <port-list> | The ports for which the neighbor information is to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors
```

To display neighbor information received via eth1 and eth2 with LLDP-MED configuration, use the command:

```
awplus# show lldp neighbors interface eth1,eth2
```

**Output** The following shows typical output.

**Example output from the show lldp neighbors command**

| LLDP Neighbor Information:                                                         |                     |                  |                         |             |            |
|------------------------------------------------------------------------------------|---------------------|------------------|-------------------------|-------------|------------|
| Total number of neighbors on these ports .... 4                                    |                     |                  |                         |             |            |
| System Capability Codes:                                                           |                     |                  |                         |             |            |
| O = Other    P = Repeater    B = Bridge                      W = WLAN Access Point |                     |                  |                         |             |            |
| R = Router   T = Telephone   C = DOCSIS Cable Device       S = Station Only        |                     |                  |                         |             |            |
| LLDP-MED Device Type and Power Source Codes:                                       |                     |                  |                         |             |            |
| 1 = Class I    3 = Class III    PSE = PoE    Both = PoE&Local    Prim = Primary    |                     |                  |                         |             |            |
| 2 = Class II   N = Network Con.   Locl = Local   Unkn = Unknown   Back = Backup    |                     |                  |                         |             |            |
| Local Port                                                                         | Neighbor Chassis ID | Neighbor Port ID | Neighbor Sys Name       | System Cap. | MED Ty Pwr |
| eth1                                                                               | 002d.3044.7ba6      | port1.0.2        | awplus                  | OPBWRCS     |            |
| eth1                                                                               | 0011.3109.e5c6      | port1.0.3        | AT-9924 switch/route... | --B-R--     |            |
| eth2                                                                               | 0000.10cf.8590      | port3            | AR-442S                 | --B-R--     |            |
| eth2                                                                               | 00ee.4352.df51      | 192.168.1.2      | Jim's desk phone        | --B--T--    | 3 PSE      |

**Parameters in the output of the show lldp neighbors command**

| Parameter           | Description                                                      |
|---------------------|------------------------------------------------------------------|
| Local Port          | Local port on which the neighbor information was received.       |
| Neighbor Chassis ID | Chassis ID that uniquely identifies the neighbor.                |
| Neighbor Port Name  | Port ID of the neighbor.                                         |
| Neighbor Sys Name   | System name of the LLDP neighbor.                                |
| Neighbor Capability | Capabilities that are supported and enabled on the neighbor.     |
| System Capability   | System Capabilities of the LLDP neighbor.                        |
| MED Device Type     | LLDP-MED Device class (Class I, II, III or Network Connectivity) |
| MED Power Source    | LLDP-MED Power Source                                            |

**Related commands** [show lldp neighbors detail](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## show lldp neighbors detail

**Overview** This command displays in detail the information received from neighbors via specified ports. If no port list is supplied, detailed neighbor information for all ports is displayed.

**Syntax** `show lldp neighbors detail [base] [dot1] [dot3] [med] [interface <port-list>]`

| Parameter   | Description                                                  |
|-------------|--------------------------------------------------------------|
| base        | Information for base TLVs.                                   |
| dot1        | Information for 802.1 TLVs.                                  |
| dot3        | Information for 803.1 TLVs.                                  |
| med         | Information for LLDP-MED TLVs.                               |
| <port-list> | The ports for which the neighbor information is to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display detailed neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors detail
```

To display detailed neighbor information received via eth1, use the command:

```
awplus# show lldp neighbors detail interface eth1
```



**Output** The following shows typical output.

**Example output from the show lldp neighbors detail command**

```
awplus#show lldp neighbors detail interface eth1
LLDP Detailed Neighbor Information:

Local eth1:
Neighbors table last updated 0 hrs 0 mins 40 secs ago
Chassis ID Type MAC address
Chassis ID 0004.cd28.8754
Port ID Type Interface alias
Port ID port1.0.6
TTL 120 (secs)
Port Description [zero length]
System Name awplus
System Description Allied Telesis router/switch, AW+ v5.4.6
System Capabilities - Supported .. Bridge, Router
 - Enabled Bridge, Router
Management Addresses 0004.cd28.8754
Port VLAN ID (PVID) 1
Port & Protocol VLAN - Supported . Yes
 - Enabled ... Yes
 - VIDs 5
VLAN Names default, vlan5
Protocol IDs 9000, 0026424203000000, 888e01, 8100,
 88090101, 00540000e302, 0800, 0806, 86dd
MAC/PHY Auto-negotiation Supported, Enabled
 Advertised Capability 1000BaseTFD, 100BaseTXFD, 100BaseTX,
 10BaseTFD, 10BaseT
 Operational MAU Type 1000BaseTFD (30)
Power Via MDI (PoE) [not advertised]
Link Aggregation Supported, Disabled
Maximum Frame Size 1522 (Octets)
LLDP-MED Device Type Network Connectivity
LLDP-MED Capabilities LLDP-MED Capabilities, Network Policy,
 Location Identification,
 Extended Power - PSE, Inventory
Network Policy [not advertised]
Location Identification [not advertised]
Extended Power Via MDI (PoE) PD
 Power Source PSE
 Power Priority High
 Power Value 4.4 Watts
Inventory Management:
 Hardware Revision X1-0
 Firmware Revision 1.1.0
 Software Revision v5.4.6
 Serial Number M1NB73008
 Manufacturer Name Allied Telesis Inc.
 Model Name x230-28GP
 Asset ID [zero length]
```

**Parameters in the output of the show lldp neighbors detail command**

| Parameter       | Description                                       |
|-----------------|---------------------------------------------------|
| Chassis ID Type | Type of the Chassis ID.                           |
| Chassis ID      | Chassis ID that uniquely identifies the neighbor. |
| Port ID Type    | Type of the Port ID.                              |

| Parameter                        | Description                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------|
| Port ID                          | Port ID of the neighbor.                                                                  |
| TTL                              | Number of seconds that the information advertised by the neighbor remains valid.          |
| Port Description                 | Port description of the neighbor's port.                                                  |
| System Name                      | Neighbor's system name.                                                                   |
| System Description               | Neighbor's system description.                                                            |
| System Capabilities (Supported)  | Capabilities that the neighbor supports.                                                  |
| System Capabilities (Enabled)    | Capabilities that are enabled on the neighbor.                                            |
| Management Addresses             | List of neighbor's management addresses.                                                  |
| Port VLAN ID (PVID)              | VLAN identifier associated with untagged or priority tagged frames for the neighbor port. |
| Port & Protocol VLAN (Supported) | Whether Port & Protocol VLAN is supported on the LLDP neighbor.                           |
| Port & Protocol VLAN (Enabled)   | Whether Port & Protocol VLAN is enabled on the LLDP neighbor.                             |
| Port & Protocol VLAN (VIDs)      | List of Port & Protocol VLAN identifiers.                                                 |
| VLAN Names                       | List of names of VLANs that the neighbor's port belongs to.                               |
| Protocol IDs                     | List of protocols that are accessible through the neighbor's port.                        |
| MAC/PHY Auto-negotiation         | Auto-negotiation configuration and status                                                 |
| Power Via MDI (PoE)              | PoE configuration and status of 802.3 Power- Via-MDI TLV                                  |
| Link Aggregation                 | Link aggregation information                                                              |
| Maximum Frame Size               | The maximum frame size capability                                                         |
| LLDP-MED Device Type             | LLDP-MED Device type                                                                      |
| LLDP-MED Capabilities            | LLDP-MED capabilities supported                                                           |

| Parameter                    | Description                       |
|------------------------------|-----------------------------------|
| Network Policy               | List of network policies          |
| Location Identification      | Location information              |
| Extended Power Via MDI (PoE) | PoE-capability and current status |
| Inventory Management         | Inventory information             |

**Related commands** [show lldp neighbors](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

# show lldp statistics

**Overview** This command displays the global LLDP statistics (packet and event counters).

**Syntax** show lldp statistics

**Mode** User Exec and Privileged Exec

**Example** To display global LLDP statistics information, use the command:  
awplus# show lldp statistics

**Output** The following shows typical output.

**Example output from the show lldp statistics command**

```
awplus# show lldp statistics
Global LLDP Packet and Event counters:

Frames: Out 345
 In 423
 In Errored 0
 In Dropped 0
TLVs: Unrecognized 0
 Discarded 0
Neighbors: New Entries 20
 Deleted Entries 20
 Dropped Entries 0
 Entry Age-outs 20
```

**Parameters in the output of the show lldp statistics command**

| Parameter                        | Description                                                                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Frames Out                       | Number of LLDPDU frames transmitted.                                                                                                               |
| Frames In                        | Number of LLDPDU frames received.                                                                                                                  |
| Frames In Errored                | Number of invalid LLDPDU frames received.                                                                                                          |
| Frames In Dropped                | Number of LLDPDU frames received and discarded for any reason.                                                                                     |
| TLVs Unrecognized                | Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.                                       |
| TLVs Discarded                   | Number of LLDP TLVs discarded for any reason.                                                                                                      |
| Neighbors New Entries            | Number of times the information advertised by neighbors has been inserted into the neighbor table.                                                 |
| Neighbors Deleted Entries        | Number of times the information advertised by neighbors has been removed from the neighbor table.                                                  |
| Neighbors Dropped Entries        | Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.            |
| Neighbors Entry Age-outs Entries | Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired. |

**Related commands** [clear lldp statistics](#)  
[show lldp statistics interface](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## show lldp statistics interface

**Overview** This command displays the LLDP statistics (packet and event counters) for specified ports. If no port list is supplied, LLDP statistics for all ports are displayed.

**Syntax** show lldp statistics interface [*<port-list>*]

| Parameter                | Description                                         |
|--------------------------|-----------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports for which the statistics are to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP statistics information for all ports, use the command:

```
awplus# show lldp statistics interface
```

To display LLDP statistics information for eth1 and eth2, use the command:

```
awplus# show lldp statistics interface eth1,eth2
```

**Output** Example output from the show lldp statistics interface command

```
awplus# show lldp statistics interface eth1,eth2

LLDP Packet and Event Counters:

eth1
 Frames: Out 27
 In 22
 In Errored 0
 In Dropped 0
 TLVs: Unrecognized 0
 Discarded 0
 Neighbors: New Entries 3
 Deleted Entries 0
 Dropped Entries 0
 Entry Age-outs 0

eth2
 Frames: Out 15
 In 18
 In Errored 0
 In Dropped 0
 TLVs: Unrecognized 0
 Discarded 0
 Neighbors: New Entries 1
 Deleted Entries 0
 Dropped Entries 0
 Entry Age-outs 0
```

**Parameters in the output of the show lldp statistics interface command**

| Parameter                 | Description                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Frames Out                | Number of LLDPDU frames transmitted.                                                                                                    |
| Frames In                 | Number of LLDPDU frames received.                                                                                                       |
| Frames In Errored         | Number of invalid LLDPDU frames received.                                                                                               |
| Frames In Dropped         | Number of LLDPDU frames received and discarded for any reason.                                                                          |
| TLVs Unrecognized         | Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.                            |
| TLVs Discarded            | Number of LLDP TLVs discarded for any reason.                                                                                           |
| Neighbors New Entries     | Number of times the information advertised by neighbors has been inserted into the neighbor table.                                      |
| Neighbors Deleted Entries | Number of times the information advertised by neighbors has been removed from the neighbor table.                                       |
| Neighbors Dropped Entries | Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources. |



| Parameter                           | Description                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Neighbors Entry<br>Age-outs Entries | Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired. |

**Related commands** [clear lldp statistics](#)  
[show lldp statistics](#)

**Command changes** Version 5.5.3-1.1: Command added to AR1050V

## show location

**Overview** Use this command to display selected location information configured on the switch.

**Syntax** `show location {civic-location|coord-location|elin-location}`  
`show location {civic-location|coord-location|elin-location}`  
`identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}`  
`show location {civic-location|coord-location|elin-location}`  
`interface <port-list>`

| Parameter      | Description                                                      |
|----------------|------------------------------------------------------------------|
| civic-location | Display civic location information.                              |
| coord-location | Display coordinate location information.                         |
| elin-location  | Display ELIN (Emergency Location Identifier Number) information. |
| <civic-loc-id> | Civic address location identifier, in the range 1 to 4095.       |
| <coord-loc-id> | Coordinate location identifier, in the range 1 to 4095.          |
| <elin-loc-id>  | ELIN location identifier, in the range 1 to 4095.                |
| <port-list>    | Ports to display information about.                              |

**Mode** User Exec and Privileged Exec

**Examples** To display a civic address location configured on eth1, use the command:

```
awplus# show location civic-location interface eth1
```

**Example output from the show location command**

```
awplus# show location civic-location interface eth1
Port ID Element Type Element Value

 [not configured]
```

To display coordinate location information configured on the identifier 1, use the command:

```
awplus# show location coord-location identifier 1
```

**Example output from the show location command**

```
awplus# show location coord-location identifier 1
ID Element Type Element Value

 1 Latitude Resolution 15 bits
 Latitude 38.8986481130123138427734375 degrees
 Longitude Resolution 15 bits
 Longitude 130.2323232293128967285156250 degrees
 Altitude Resolution 10 bits
 Altitude 2.500000000 meters
 Map Datum WGS 84
```

The coordinate location information displayed may differ from the information entered because it is stored in binary format. For more information, see the [location coord-location configuration](#) command.

To display all ELIN location information configured on the switch, use the command:

```
awplus# show location elin-location
```

**Example output from the show location elin-location command**

```
awplus# show location elin-location
ID ELIN

 1 1234567890
 2 5432154321
```

**Related commands**

- [location civic-location identifier](#)
- [location civic-location configuration](#)
- [location coord-location identifier](#)
- [location coord-location configuration](#)
- [location elin-location](#)

**Command changes**

- Version 5.5.3-1.1: Command added to AR1050V
- Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

# 37

## Mail (SMTP) Commands

- Contents**
- **Introduction** on page 1913
  - **debug mail** on page 1914
  - **delete mail** on page 1915
  - **mail** on page 1916
  - **mail from** on page 1918
  - **mail smtpserver** on page 1919
  - **mail smtpserver authentication** on page 1920
  - **mail smtpserver port** on page 1922
  - **mail smtpserver tls** on page 1924
  - **show counter mail** on page 1926
  - **show mail** on page 1927
  - **undebug mail** on page 1928

# 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**.

# 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 <b>show mail</b> command to display this for an item of mail. |
| all       | Delete all the mail in the queue.                                                                        |

**Mode** Privileged Exec

**Examples** To delete the unique mail item "20060912142356.1234" from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

**Related commands**

- debug mail**
- mail**
- mail from**
- mail smtpserver**
- show mail**

# mail

**Overview** This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the **mail from** command and a mail server using the **mail smtpserver** command.

**Syntax** mail [to <to>] [subject <subject>] [file <filename>]

| Parameter | Description                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------|
| to        | The email recipient.                                                                             |
|           | <to> Email address.                                                                              |
| subject   | Description of the subject of this email. Use quote marks when the subject text contains spaces. |
|           | <subject> String.                                                                                |
| file      | File to insert as text into the message body.                                                    |
|           | <filename> String.                                                                               |

**Mode** Privileged Exec



**Usage notes** When you use the **mail** command you can use parameter substitutions in the subject field. The following table lists the parameters that can be substituted and their descriptions:

| Parameter Description |                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------|
| <%N>                  | When this parameter is specified, the %N is replaced by the host name of your device.                                  |
| <%S>                  | When this parameter is specified, the %S is replaced by the serial number of your device.                              |
| <%D><%L><             | 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** The following shows typical output.

**Example output from show mail:**

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : 1.2.3.4
Host Name : admin@example.com
Authentication : crammd5
Username : admin
Debug : Disabled

awplus#show running-config
!
mail smtpserver authentication plain username admin password 8
aF0a9pkjbmXGfl6TlSk/GakeIK5tMYN6LqMYT8Ia2qw=
!
```

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [mail smtpserver port](#)
- [show counter mail](#)
- [show mail](#)

**Command changes** Version 5.4.8-1.1: command added

# mail smtpserver port

**Overview** Use this command to configure the SMTP mail client/server communication port.

Use the **no** variant of this command to remove the configured port and set it back to the default port.

**Syntax** mail smtpserver port <port>  
no mail smtpserver port

| Parameter | Description                           |
|-----------|---------------------------------------|
| <port>    | Port number from the range 1 to 65535 |

**Default** The default port value is 25 if TLS is not enabled for the SMTP server, 587 if TLS is enabled with STARTTLS, and 465 if TLS is enabled with SMTPS.

**Mode** Global Configuration

**Examples** To configure the mail server communication over port 587, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver port 587
```

To revert to the default SMTP mail server communication port, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver port
```

**Output** The following shows typical output.

**Example output from show mail:**

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : 10.24.165.4
Host Name : admin@example.com
Authentication : plain
Username : admin
Port : 587
Use TLS : STARTTLS
Debug : Disabled

awplus#show running-config
!
mail smtpserver port 587
!
```

- Related commands

debug mail

delete mail

mail

mail from

mail smtpserver

mail smtpserver tls

show counter mail

show mail

Command changes

Version 5.4.8-1.1: command added

# mail smtpserver tls

**Overview** Use this command to configure the device to send emails over a TLS connection to the SMTP server instead of sending in clear-text. If the SMTP server does not support receiving emails over a TLS connection, sending emails from the device will fail.

Use the **no** variant of this command to configure the device to send emails over an unencrypted TCP connection (clear text).

**Syntax** mail smtpserver tls [starttls|smtps]  
no mail smtpserver tls

| Parameter | Description                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|
| starttls  | The connection starts as clear-text SMTP first and then the client establishes a TLS connection using the STARTTLS extension. |
| smtps     | Use a TLS connection from the start.                                                                                          |

**Default** By default, TLS is disabled and the device sends emails in clear-text.

**Mode** Global Configuration

**Examples** To send emails to the SMTP server over a TLS connection that will be established by the STARTTLS method, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls starttls
```

To send emails to the SMTP server over a TLS connection from the beginning, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls smtps
```

To send emails to the SMTP server in clear text, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver tls
```

**Related commands** [mail](#)  
[show mail](#)  
[mail smtpserver](#)  
[mail smtpserver port](#)  
[mail smtpserver authentication](#)



**Command changes** Version 5.5.3-0.1: command added

# show counter mail

**Overview** This command displays the mail counters.

**Syntax** show counter mail

**Mode** User Exec and Privileged Exec

**Example** To show the emails in the queue use the command:

```
awplus# show counter mail
```

**Output** The following shows typical output.

## Example output from the show counter mail command

```
Mail Client (SMTP) counters
Mails Sent 2
Mails Sent Fails 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** The following shows typical output.

**Example output from the show mail command:**

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : example.net
Host Name : test@example.com
Authentication : login
Username : admin
Port : 587
Use TLS : STARTTLS
Debug : Disabled

Messages

There is no mail in the queue.
```

**Related commands**

- [delete mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [mail smtpserver tls](#)
- [show counter mail](#)
- [mail smtpserver port](#)
- [undebug mail](#)

# undebug mail

**Overview** This command applies the functionality of the no **debug mail**.

# 38

## RMON Commands

- Contents**
- **Introduction** on page 1930
  - **rmon alarm** on page 1931
  - **rmon collection history** on page 1936
  - **rmon collection stats** on page 1938
  - **rmon event** on page 1939
  - **show rmon alarm** on page 1940
  - **show rmon event** on page 1941
  - **show rmon history** on page 1942
  - **show rmon statistics** on page 1944

# Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see the [RMON Feature Overview and Configuration Guide](#).

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

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

## rmon alarm

**Overview** Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the **rmon event** command.

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

**NOTE:**

*You can only configure alarms for Eth, tunnel and switch port interfaces.*

### Syntax User-defined alarm:

```
rmon alarm <alarm-index> <oid.index> interval <1-2147483647>
{delta|absolute} rising-threshold <1-2147483647> event <rising-
event-index> falling-threshold <1-2147483647> event <falling-
event-index> [alarmstartup {1|2|3}] [owner <owner>]
```

### Eventwatch alarm, do not use (used by Vista Manager EX only):

```
rmon alarm <alarm-index> <oid.index> interval <1-4294967295>
{delta|absolute} rising-threshold <1-2147483647> event
eventwatch falling-threshold <1-2147483647> event eventwatch
[owner <owner>]
```

```
no rmon alarm <alarm-index>
```

| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <alarm-index>                      | Alarm entry index value from the range 1 to 65535 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <oid.index>                        | <p>The variable SNMP MIB Object Identifier (OID) name to be monitored, for either etherStats or etherHistory entries. The entries can be either of the following formats:</p> <ul style="list-style-type: none"> <li>- etherStatsEntry.&lt;field&gt;.&lt;stats-index&gt; or etherHistoryEntry.&lt;field&gt;.&lt;history-index&gt;, or</li> <li>- etherStatsFieldName.&lt;stats-index&gt; or etherHistoryFieldName.&lt;history-index&gt;.</li> </ul> <p>To define the &lt;stats-index&gt;, use the <b>rmon collection stats</b> command.</p> <p>To define the &lt;history-index&gt;, use the <b>rmon collection history</b> command.</p> |
| interval<br><1-2147483647>         | Polling interval in seconds from the range 1 to 2147483647.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| delta                              | The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| absolute                           | The RMON MIB alarmSampleType: the value of the monitored MIB object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| rising-threshold<br><1-2147483647> | Rising threshold value of the alarm entry in seconds from the range 1 to 2147483647.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <rising-event-index>               | From the range 1 to 65535 seconds. The event to be triggered when the monitored object value reaches the rising threshold value. This is the event index of an event specified by the <b>rmon event</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| eventwatch                         | The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



| Parameter                           | Description                                                                                                                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | monitoring tool. Do not use this parameter; use the <i>&lt;rising-event-index&gt;</i> parameter instead.                                                                                                                               |
| falling-threshold<br><1-2147483647> | Falling threshold value of the alarm entry in seconds from the range 1 to 2147483647.                                                                                                                                                  |
| <falling-event-index>               | From the range 1 to 65535 seconds. The event to be triggered when the monitored object value reaches the falling threshold value. This is an event index of an event specified by the <b>rmon event</b> command.                       |
| eventwatch                          | The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and monitoring tool. Do not use this parameter; use the <i>&lt;rising-event-index&gt;</i> parameter instead. |
| alarmstartup {1 2 3}                | Whether RMON can trigger a falling alarm (1), a rising alarm (2) or either (3) when you first start monitoring. See the Usage section for more information.<br><br>The default is setting 3 (either).                                  |
| owner <owner>                       | Arbitrary owner name to identify the alarm entry.                                                                                                                                                                                      |

**Default** By default, there are no alarms.

**Mode** Global Configuration

**Usage notes** RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The **alarmstartup** parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that you specify the SNMP MIB Object Identifier (OID) as a dotted decimal value, using one of the following forms:

- etherStatsEntry.<field>.<stats-index> or etherHistoryEntry.<field>.<history-index>. For example, etherHistoryEntry.8.8
- or, etherStatsFieldName.<stats-index> or etherHistoryFieldName.<history-index>. For example, etherHistoryMulticastPkts.8

If you enter the first form (etherHistoryEntry.8.8), the device will save it as the second form (etherHistoryMulticastPkts.8) in the running-config.

**Example** To configure an alarm to:

- monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the **rmon collection stats** command)
- and trigger event 2 (defined by the **rmon event** command) when the change reaches the rising threshold 400
- and trigger event 3 when it reaches the falling threshold 200
- and identify this alarm as belonging to the user with username Maria

use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60
delta rising-threshold 400 event 2 falling-threshold 200 event
3 alarmstartup 3 owner maria
```

To configure an alarm that:

- every 10 seconds, checks the number of multicast packets
- in the latest history control table entry controlled by history-index 8
- to see if the number of packets has increased to 15 or dropped to 5
- and if it has, triggers event 10

use either of the following commands:

```
awplus(config)# rmon alarm 56 etherHistoryMulticastPkts.8
interval 10 absolute rising-threshold 15 event 10 falling-
threshold 5 event 10
```

```
awplus(config)# rmon alarm 56 etherHistoryEntry.8.8 interval 10
absolute rising-threshold 15 event 10 falling-threshold 5 event
10
```

**Related commands** [rmon collection history](#)  
[rmon collection stats](#)  
[rmon event](#)

## rmon collection history

**Overview** Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the **no** variant of this command to remove the specified history control configuration.

**NOTE:** A history can only be collected for tunnels, eth interfaces and switch port interfaces.

**Syntax** `rmon collection history <history-index> [buckets <1-65535>]  
[interval <1-3600>] [owner <owner>]  
no rmon collection history <history-index>`

| Parameter         | Description                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------|
| <history-index>   | A unique RMON history control entry index value from the range 1 to 65535.                           |
| buckets <1-65535> | Number of requested buckets to store snapshots from the range 1 to 65535. The default is 50 buckets. |
| interval <1-3600> | Polling interval in seconds. Default 1800 second polling interval from the range 1 to 3600.          |
| owner <owner>     | Owner name to identify the entry.                                                                    |

**Default** The default interval is 1800 seconds and the default number of buckets is 50.

**Mode** Interface Configuration

**Example** To create a history statistics control group with ID 200 to store 500 snapshots with an interval of 600 seconds, use the commands:

```
awplus# configure terminal
awplus(config-if)# rmon collection history 200 buckets 500
interval 600 owner herbert
```

To disable the history statistics control group, use the commands:

```
awplus# configure terminal
awplus(config-if)# no rmon collection history 200
```

**Related commands** [rmon alarm](#)  
[rmon collection stats](#)  
[rmon event](#)

## rmon collection stats

**Overview** Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the **no** variant of this command to stop collecting RMON statistics on this switch port.

**NOTE:** *Statistics can only be collected for tunnels, eth interfaces and switch port interfaces.*

**Syntax** `rmon collection stats <collection-index> [owner <owner>]`  
`no rmon collection stats <collection-index>`

| Parameter          | Description                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <collection-index> | Give this collection of statistics an index number to uniquely identify it. This is the index to use to access the statistics collected for this switch port. Use a number in the range of 1 to 65535. |
| owner <owner>      | An arbitrary owner name to identify this statistics collection entry.                                                                                                                                  |

**Default** RMON statistics are not enabled by default.

**Mode** Interface Configuration

**Example** To enable the collection of RMON statistics with a statistics index of 200, use the commands:

```
awplus# configure terminal
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config-if)# no rmon collection stats 200
```

**Related commands** [rmon alarm](#)  
[rmon collection history](#)  
[rmon event](#)

## rmon event

**Overview** Use this command to create an event definition for a log or a trap or both. Then you can use this event index in the **rmon alarm** command to indicate whether to send an SNMP trap or log message (or both) when an alarm is triggered.

Use the **no** variant of this command to remove the event definition.

**Syntax**

```
rmon event <event-index> [description <description>|owner <owner>| trap <trap>]
rmon event <event-index> [log [description <description>|owner <owner>|trap <trap>]]
rmon event <event-index> [log trap [description <description>|owner <owner>]]
no rmon event <event-index>
```

| Parameter                | Description                               |
|--------------------------|-------------------------------------------|
| <event-index>            | <1-65535> Unique event entry index value. |
| log                      | Log event type.                           |
| trap                     | Trap event type.                          |
| log trap                 | Log and trap event type.                  |
| description<description> | Event entry description.                  |
| owner <owner>            | Owner name to identify the entry.         |

**Default** No event is configured by default.

**Mode** Global Configuration

**Example** To create an event definition with an index of 299 for a log, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To remove the event definition, use the command:

```
awplus# configure terminal
awplus(config)# no rmon event 299
```

**Related commands** **rmon alarm**

# show rmon alarm

**Overview** Use this command to display the alarms and threshold configured for the RMON probe.

**Syntax** show rmon alarm

**Mode** User Exec and Privileged Exec

**Example** To display the alarms and threshold, use this command:  
awplus# show rmon alarm

**Related commands** [rmon alarm](#)



# show rmon event

**Overview** Use this command to display the events configured for the RMON probe.

**Syntax** show rmon event

**Mode** User Exec and Privileged Exec

**Output** The following shows typical output.

## Example output from the show rmon event command

```
awplus#sh rmon event
event Index = 787
 Description TRAP
 Event type log & trap
 Event community name gopher
 Last Time Sent = 0
 Owner RMON_SNMP

event Index = 990
 Description TRAP
 Event type trap
 Event community name teabo
 Last Time Sent = 0
 Owner RMON_SNMP
```

**NOTE:** The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Example** To display the events configured for the RMON probe, use this command:

```
awplus# show rmon event
```

**Related commands** [rmon event](#)

# show rmon history

**Overview** Use this command to display the parameters specified on all the currently defined RMON history collections on the device.

**Syntax** show rmon history

**Mode** User Exec and Privileged Exec

**Output** The following shows typical output.

## Example output from the show rmon history command

```
awplus#sh rmon history
 history index = 56
 data source ifindex = 4501
 buckets requested = 34
 buckets granted = 34
 Interval = 2000
 Owner Andrew

 history index = 458
 data source ifindex = 5004
 buckets requested = 400
 buckets granted = 400
 Interval = 1500
 Owner trev
=====
```

**NOTE:** The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Example** To display the parameters specified on all the currently defined RMON history collections, us the commands:

```
awplus# show rmon history
```

**Related commands** [rmon collection history](#)

# show rmon statistics

**Overview** Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

**Syntax** show rmon statistics

**Mode** User Exec and Privileged Exec

**Example** To display the current values of the statistics for all the RMON statistics collections, use the commands:

```
awplus# show rmon statistics
```

**Output** The following shows typical output.

## Example output from the show rmon statistics command

```
awplus#show rmon statistics
 rmon collection index 45
 stats->ifindex = 4501
 input packets 1279340, bytes 85858960, dropped 00, multicast packets 1272100
 output packets 7306090, bytes 268724, multicast packets 7305660 broadcast
 packets 290
 rmon collection index 679
 stats->ifindex = 5013
 input packets 00, bytes 00, dropped 00, multicast packets 00
 output packets 8554550, bytes 26777324, multicast packets 8546690 broadcast
 packets 7720
```

**NOTE:** The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Related commands** [rmon collection stats](#)

# 39

## Secure Shell (SSH) Commands

- Contents**
- **Introduction** on page 1947
  - **banner login (SSH)** on page 1948
  - **clear ssh** on page 1949
  - **crypto key destroy hostkey** on page 1950
  - **crypto key destroy userkey** on page 1951
  - **crypto key generate hostkey** on page 1952
  - **crypto key generate userkey** on page 1954
  - **crypto key pubkey-chain knownhosts** on page 1956
  - **crypto key pubkey-chain userkey** on page 1958
  - **debug ssh client** on page 1960
  - **debug ssh server** on page 1961
  - **service ssh** on page 1962
  - **show banner login** on page 1964
  - **show crypto key hostkey** on page 1965
  - **show crypto key pubkey-chain knownhosts** on page 1967
  - **show crypto key pubkey-chain userkey** on page 1969
  - **show crypto key userkey** on page 1971
  - **show running-config ssh** on page 1973
  - **show ssh** on page 1975
  - **show ssh client** on page 1978
  - **show ssh server** on page 1979
  - **show ssh server allow-users** on page 1982
  - **show ssh server deny-users** on page 1983
  - **ssh** on page 1984
  - **ssh client** on page 1987
  - **ssh client allow-legacy-ssh-rsa** on page 1990
  - **ssh client vrf** on page 1991
  - **ssh server** on page 1992
  - **ssh server allow-legacy-ssh-rsa** on page 1994
  - **ssh server allow-users** on page 1995
  - **ssh server authentication** on page 1997
  - **ssh server deny-users** on page 1999
  - **ssh server max-auth-tries** on page 2001
  - **ssh server resolve-host** on page 2002
  - **ssh server scp** on page 2003
  - **ssh server secure-algs** on page 2004
  - **ssh server secure-ciphers** on page 2005

- **ssh server secure-hostkey** on page 2006
- **ssh server secure-kex** on page 2007
- **ssh server secure-mac** on page 2008
- **ssh server sftp** on page 2009
- **ssh server tcpforwarding** on page 2010
- **ssh server vrf** on page 2011
- **undebug ssh client** on page 2012
- **undebug ssh server** on page 2013

# 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**.

## 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.

**Syntax** `crypto key destroy hostkey {dsa|ecdsa|ed25519|rsa|rsa1}`

| Parameters | Description                                                                                                                                                                          |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dsa        | Deletes the existing DSA public and private keys.                                                                                                                                    |
| ecdsa      | Deletes the existing ECDSA public and private keys.                                                                                                                                  |
| ed25519    | Deletes the existing Ed25519 public and private keys.                                                                                                                                |
| rsa        | Deletes the existing RSA public and private keys that were configured for SSH version 2 connections.                                                                                 |
| rsa1       | Deletes the existing RSA public and private keys that were configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported. |

**Mode** Global Configuration

**Example** To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

**Related commands** [crypto key generate hostkey](#)  
[service ssh](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added

# crypto key destroy userkey

**Overview** This command destroys the existing public and private keys of an SSH user configured on the device.

**Syntax** `crypto key destroy userkey <username> {dsa|ecdsa|ed25519|rsa|rsa1}`

| Parameters | Description                                                                                                                                                                            |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| dsa        | Deletes the existing DSA userkey.                                                                                                                                                      |
| ecdsa      | Deletes the existing ECDSA userkey.                                                                                                                                                    |
| ed25519    | Deletes the existing Ed25519 userkey.                                                                                                                                                  |
| rsa        | Deletes the existing RSA userkey that was configured for SSH version 2 connections.                                                                                                    |
| rsa1       | Deletes the existing RSA userkey that was configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported.                    |

**Mode** Global Configuration

**Example** To destroy the RSA user key for the SSH user remoteuser, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

**Related commands**

- [crypto key generate hostkey](#)
- [crypto key generate userkey](#)
- [show ssh](#)
- [show crypto key hostkey](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added

# crypto key generate hostkey

**Overview** This command generates public and private keys for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using Ed25519 with a keysize of 256, ECDSA with a curve length of 384, and RSA with a 3072-bit key.

If you need a key with different parameters than this, you can use this command to generate that key before you enable the SSH server. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax** `crypto key generate hostkey rsa [<1024-16384>]`  
`crypto key generate hostkey ecdsa [<256|384|521>]`  
`crypto key generate hostkey ed25519`

| Parameters    | Description                                       |
|---------------|---------------------------------------------------|
| rsa           | Creates an RSA hostkey.                           |
| ecdsa         | Creates an ECDSA hostkey.                         |
| ed25519       | Creates an Ed25519 hostkey with a keysize of 256. |
| <1024-16384>  | The length in bits of the generated key.          |
| <256 384 521> | The ECDSA key size in bits.                       |

**Default** The default key length for RSA is 3072 bits.  
The default key size for ECDSA is 384 bits.

**Mode** Global Configuration

**Examples** To generate an RSA host key that is 4096 bits in length, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# crypto key generate hostkey rsa 4096
```

To generate an ECDSA host key with an elliptic curve size of 521 bits, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# crypto key generate hostkey ecdsa 521
```

To generate an Ed25519 host key with a keysize of 256, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# crypto key generate hostkey ed25519
```

**Related commands** [crypto key destroy hostkey](#)  
[service ssh](#)  
[show crypto key hostkey](#)

**Command changes** Version 5.5.5-1.1: default RSA key length increased to 3072  
Version 5.5.2-2.1: **ed25519** parameter added  
Version 5.5.2-0.1: changes to key length and key size ranges and defaults  
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# crypto key generate userkey

**Overview** This command generates public and private keys for an SSH user using an RSA, ECDSA, or ED25519 cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax** `crypto key generate userkey <username> rsa [<1024-16384>]`  
`crypto key generate userkey <username> ecdsa [<256|384|521>]`  
`crypto key generate userkey <username> ed25519`

| Parameters    | Description                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username>    | Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| rsa           | Creates an RSA userkey.                                                                                                                                                                  |
| ecdsa         | Creates an ECDSA userkey.                                                                                                                                                                |
| ed25519       | Creates an Ed25519 userkey with a keysize of 256.                                                                                                                                        |
| <1024-16384>  | The length in bits of the generated key. The default is 2048 bits.                                                                                                                       |
| <256 384 521> | The ECDSA key size in bits. The default is 384.                                                                                                                                          |

**Default** The default key length for RSA is 2048 bits.  
The default key size for ECDSA is 384 bits.

**Mode** Global Configuration

**Examples** To generate a 4096-bit RSA user key for SSH version 2 connections for the user 'bob', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 4096
```

To generate an ECDSA user key of key size 521 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ecdsa 521
```

To generate an Ed25519 user key of key size 256 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ed25519
```

**Related commands** [crypto key pubkey-chain userkey](#)  
[show crypto key userkey](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added  
Version 5.5.2-0.1: changes to key length and key size ranges and defaults  
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# crypto key pubkey-chain knownhosts

**Overview** This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

**Syntax** `crypto key pubkey-chain knownhosts [ip|ipv6] <hostname> [ecdsa|rsa]`  
`no crypto key pubkey-chain knownhosts <1-65535>`

**Syntax (VRF-lite)** `crypto key pubkey-chain knownhosts [vrf <vrf-name>] [ip|ipv6] <hostname> [ecdsa|rsa]`  
`no crypto key pubkey-chain knownhosts [vrf <vrf-name>] <1-65535>`

| Parameter                     | Description                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vrf</code>              | Apply this command to the specified VRF instance.                                                                                          |
| <code>&lt;vrf-name&gt;</code> | The VRF instance name                                                                                                                      |
| <code>ip</code>               | Keyword used prior to specifying an IPv4 address                                                                                           |
| <code>ipv6</code>             | Keyword used prior to specifying an IPv6 address                                                                                           |
| <code>&lt;hostname&gt;</code> | IPv4/IPv6 address or hostname of a remote server in the format a.b.c.d for an IPv4 address, or in the format x:x::x:x for an IPv6 address. |
| <code>ecdsa</code>            | Specify the ECDSA public key of the server to be added to the known host database.                                                         |
| <code>rsa</code>              | Specify the RSA public key of the server to be added to the known host database.                                                           |
| <code>&lt;1-65535&gt;</code>  | Specify a key identifier when removing a key using the <b>no</b> parameter.                                                                |

**Default** If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.



**Mode** Privilege Exec

**Usage notes** This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

**Examples** To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

**Examples (VRF-lite)** To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 in VRF 'red' to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts vrf red 192.0.2.11
```

To delete the second entry in the known host database in VRF 'red', use the command:

```
awplus# no crypto key pubkey-chain knownhosts vrf red 2
```

**Validation** **show crypto key pubkey-chain knownhosts**  
**Commands**

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# 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><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
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aw2fc0w1TStpb9J20bWluhnUC768EoWhyP
+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/
pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=

awplus# configure terminal
awplus(config)# crypto key pubkey-
chain userkey joeType CNTRL/D to
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aw2fc0w1TStpb9J20bWluhnUC768Eo
+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/
pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=control-D
awplus(config)#
```

To add a public key for the user graydon from the file key.pub, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey graydon key.pub
```

To add a public key for the user tamara from the terminal, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey tamara
```

and enter the key. Use Ctrl+D to finish.

To remove the first key entry from the public key chain of the user john, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain userkey john 1
```

**Related commands** [show crypto key pubkey-chain userkey](#)

# debug ssh client

**Overview** This command enables the SSH client debugging facility. When enabled, any SSH, SCP and SFTP client sessions send diagnostic messages to the login terminal.

The **no** variant of this command disables the SSH client debugging facility. This stops the SSH client from generating diagnostic debugging message.

**Syntax** debug ssh client [brief|full]  
no debug ssh client

| Parameter | Description               |
|-----------|---------------------------|
| brief     | Enables brief debug mode. |
| full      | Enables full debug mode.  |

**Default** SSH client debugging is disabled by default.

**Mode** Privileged Exec and Global Configuration

**Examples** To start SSH client debugging, use the command:

```
awplus# debug ssh client
```

To start SSH client debugging with extended output, use the command:

```
awplus# debug ssh client full
```

To disable SSH client debugging, use the command:

```
awplus# no debug ssh client
```

**Related commands** [debug ssh server](#)  
[show ssh client](#)  
[undebug ssh client](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V

# debug ssh server

**Overview** This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

**Syntax** debug ssh server [brief|full]  
no debug ssh server

| Parameter | Description               |
|-----------|---------------------------|
| brief     | Enables brief debug mode. |
| full      | Enables full debug mode.  |

**Default** SSH server debugging is disabled by default.

**Mode** Privileged Exec and Global Configuration

**Examples** To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

**Related commands** [show ssh server](#)  
[undebug ssh server](#)

## service ssh

**Overview** Use this command to enable the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key.

If you need a key with different parameters than this, you can use the **crypto key generate hostkey** command to generate that key before you enable the SSH server.

Use the **no** variant of this command to disable the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the **clear ssh** command.

**Syntax** service ssh [ip|ipv6]  
no service ssh [ip|ipv6]

**Default** The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

**Mode** Global Configuration

**Examples** To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

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

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

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

**Related commands**

- [\*\*crypto key generate hostkey\*\*](#)
- [\*\*show running-config ssh\*\*](#)
- [\*\*show ssh server\*\*](#)
- [\*\*ssh server allow-users\*\*](#)
- [\*\*ssh server deny-users\*\*](#)

**Command changes** Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# show banner login

**Overview** This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

**Syntax** show banner login

**Mode** User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

**Example** To display the current login banner message, use the command:

```
awplus# show banner login
```

**Related commands** [banner login \(SSH\)](#)



# show crypto key hostkey

**Overview** This command displays the public keys generated on the device for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using Ed25519 with a keysize of 256, ECDSA with a curve length of 384, and RSA with a 3072-bit key.

The private key remains on the device secretly. The public key is copied to SSH clients to identify the server. This command displays the public key.

**Syntax** show crypto key hostkey [ecdsa|ed25519|rsa]

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| ecdsa     | Displays the ECDSA algorithm public key.                             |
| ed25519   | Displays the Ed25519 algorithm public key.                           |
| rsa       | Displays the RSA algorithm public key for SSH version 2 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** The following shows typical output.

**Example output from the show crypto key hostkey command**

| Type                                               | Bits | Fingerprint |
|----------------------------------------------------|------|-------------|
| -----                                              |      |             |
| rsa                                                | 2048 |             |
| SHA256:K7hes31yK6uuN04sprZtFcyX9sUuXP42gou110348n8 |      |             |
| ecdsa                                              | 384  |             |
| SHA256:qhBXhkcUCC6FKwy3+pRlrRs0NtZhibreqDv9vLs9tVQ |      |             |
| ed25519                                            | 256  |             |
| SHA256:S8e/9WjCZHsUTEAHMYkIKEoxusmrLOIGe2oSs34clbA |      |             |

**Parameters in output of the show crypto key hostkey command**

| Parameter   | Description                         |
|-------------|-------------------------------------|
| Type        | Algorithm used to generate the key. |
| Bits        | Length in bits of the key.          |
| Fingerprint | Checksum value for the public key.  |

**Related commands** [crypto key destroy hostkey](#)  
[crypto key generate hostkey](#)

# show crypto key pubkey-chain knownhosts

**Overview** This command displays the list of public keys maintained in the known host database on the device.

**Syntax** show crypto key pubkey-chain knownhosts [<1-65535>]

**Syntax (VRF-lite)** show crypto key pubkey-chain knownhosts [vrf <vrf-name>|global] [<1-65535>]

| Parameter  | Description                                                                                |
|------------|--------------------------------------------------------------------------------------------|
| global     | When VRF-lite is configured, apply the command to the global routing and forwarding table. |
| vrf        | Apply the command to the specified VRF instance.                                           |
| <vrf-name> | The name of the VRF instance.                                                              |
| <1-65535>  | Key identifier for a specific key. Displays the public key of the entry if specified.      |

**Default** Display all keys.

**Mode** User Exec, Privileged Exec and Global Configuration

**Usage** When VRF-lite is configured:

- If **vrf** is specified, this command displays the known host database from the specified VRF instance.
- If **global** is specified, this command displays the known host database from the global routing environment.
- If neither **vrf** nor **global** is specified, this command displays the known host database from the global routing environment and each configured VRF.

For more information about VRF, see the [VRF Lite Feature Overview and Configuration Guide](#).

**Examples** To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

**Output** The following shows typical output.

**Example output from the show crypto key public-chain knownhosts command**

| No | Hostname                                 | Type | Fingerprint                                     |
|----|------------------------------------------|------|-------------------------------------------------|
| 1  | 172.16.23.1                              | rsa  | c8:33:b1:fe:6f:d3:8c:81:4e:f7:2a:aa:a5:be:df:18 |
| 2  | 172.16.23.10                             | rsa  | c4:79:86:65:ee:a0:1d:a5:6a:e8:fd:1d:d3:4e:37:bd |
| 3  | 5ffe:1053:ac21:ff00:0101:bcd:f:ffff:0001 | rsa1 | af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57 |

**Parameters in the output of the show crypto key public-chain knownhosts command**

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| No          | Number ID of the key.                   |
| Hostname    | Host name of the known SSH server.      |
| Type        | The algorithm used to generate the key. |
| Fingerprint | Checksum value for the public key.      |

**Related commands** [crypto key pubkey-chain knownhosts](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V  
Version 5.4.6-2.1: VRF-lite support added for AR-Series devices

# show crypto key pubkey-chain userkey

**Overview** This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

**Syntax** show crypto key pubkey-chain userkey <username> [<1-65535>]

| Parameter  | Description                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| <1-65535>  | Key identifier for a specific key.                                                                                                                                                                   |

**Default** Display all keys.

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the public keys for the user manager that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

**Output** The following shows typical output.

**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 |

**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** [crypto key pubkey-chain userkey](#)  
**commands**

# 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** The following shows typical output.

## 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 |

## 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** The following shows typical output.

**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
```

**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.                                      |
| 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** The following shows typical output.

**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 |  |

**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.                                                                           |                                                 |
| 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.                          |

| Parameter | Description                                                           |
|-----------|-----------------------------------------------------------------------|
| Filename  | Local filename of the file that the user is downloading or uploading. |

**Related** [clear ssh](#)  
**commands**

# show ssh client

**Overview** This command displays the current configuration of the Secure Shell client.

**Syntax** show ssh client

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the current configuration for SSH clients on the login shell, use the command:

```
awplus# show ssh client
```

**Output** The following shows typical output.

## Example output from the show ssh client command

```
Secure Shell Client Configuration

Port : 22
Version : 2,1
Connect Timeout : 30 seconds
Session Timeout : 0 (off)
Debug : NONE
```

## Parameters in the output of the show ssh client command

| Parameter       | Description                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port            | SSH server TCP port where the SSH client connects to. The default is port 22.                                                                               |
| Version         | SSH server version, either "2" or "2,1". From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.                                            |
| Connect Timeout | Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout. |
| Debug           | Whether debugging is active on the client.                                                                                                                  |

**Related commands** [show ssh server](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V

# show ssh server

**Overview** This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

**Syntax** show ssh server

**Mode** User Exec, Privileged Exec, and Global Configuration

**Example** To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

**Output** The following shows typical output.

**Example output from the show ssh server command**

```
Secure Shell Server Configuration

SSH Server : Enabled
Protocol : IPv4,IPv6
Port : 22
Version : 2
Services : scp, sftp
User Authentication : publickey, password
Resolve Hosts : Disabled
Session Timeout : 0 (Off)
Login Timeout : 60 seconds
Maximum Authentication Tries : 6
Maximum Startups : 10
Debug : NONE
Ciphers : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX : curve25519-sha256@libssh.org,
 ecdh-sha2-nistp256,ecdh-sha2-nistp384,
 ecdh-sha2-nistp521,
 diffie-hellman-group-exchange-sha256,
 diffie-hellman-group-exchange-sha1,
 diffie-hellman-group14-sha1
```

**Parameters in the output of the show ssh server command**

| Parameter           | Description                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH Server          | Whether the Secure Shell server is enabled or disabled.                                                                                                                              |
| Port                | TCP port where the Secure Shell server listens for connections. The default is port 22.                                                                                              |
| Version             | SSH server version; either '2' or '2.1'. From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.                                                                     |
| Services            | List of the available Secure Shell services; one or more of SHELL, SCP or SFTP.                                                                                                      |
| User Authentication | List of available authentication methods.                                                                                                                                            |
| Login Timeout       | Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches.                       |
| Idle Timeout        | Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off. |
| Maximum Startups    | The maximum number of concurrent connections that are waiting authentication. The default is 10.                                                                                     |
| Debug               | Whether debugging is active on the server.                                                                                                                                           |



| Parameter | Description                                |
|-----------|--------------------------------------------|
| Ciphers   | List of ciphers permitted.                 |
| KEX       | List of available Key Exchange algorithms. |

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

# 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** The following shows typical output.

## Example output from the show ssh server allow-users command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| -----    | -----                     |
| awplus   | 192.168.*                 |
| john     |                           |
| manager  | *.alliedtelesis.com       |

## 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** The following shows typical output.

## Example output from the show ssh server deny-users command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| -----    | -----                     |
| john     | *.b-company.com           |
| manager  | 192.168.2.*               |

## Parameters in the output of the show ssh server deny-user command

| Parameter                 | Description                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                  | The user that this rule applies to.                                                                                                                                                     |
| Remote Hostname (pattern) | IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts. |

**Related commands** [ssh server allow-users](#)  
[ssh server deny-users](#)

## ssh

**Overview** Use this command to initiate a Secure Shell connection to a remote SSH server.

If the server requests a password to login, you need to type in the correct password at the "Password:" prompt.

An SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

**NOTE:** A hostname specified with SSH cannot begin with a hyphen (-) character.

**Syntax** `ssh [ip|ipv6] [user <username>|port <1-65535>|version 2]  
<remote-device> [<command>]`

**Syntax (VRF-lite)** `ssh vrf <vrf-name> [ip|ipv6] [user <username>|port <1-65535>|  
version 2] <remote-device> [<command>]`

| Parameter       | Description                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf             | Apply the command to the specified VRF instance. When using VRF, specifying a VRF name means the command will apply to that VRF instance, and not specifying a VRF name means the command will apply to the global VRF.                      |
| <vrf-name>      | The name of the VRF instance.                                                                                                                                                                                                                |
| ip              | Specify IPv4 SSH.                                                                                                                                                                                                                            |
| ipv6            | Specify IPv6 SSH.                                                                                                                                                                                                                            |
| user            | Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.                                                                     |
|                 | <username> User name to login on the remote server.                                                                                                                                                                                          |
| port            | SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Otherwise, the client port configured by "ssh client" command or the default TCP port (22) is used.                     |
|                 | <1-65535> TCP port.                                                                                                                                                                                                                          |
| version         | SSH client version. From 5.5.1-1.1 onwards, SSH only supports version 2.                                                                                                                                                                     |
| <remote-device> | IPv4/IPv6 address or hostname of a remote server. The address is in the format A.B.C.D for an IPv4 address, or in the format X:X::X:X for an IPv6 address. Note that a hostname specified with SSH cannot begin with a hyphen (-) character. |
| <command>       | A command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.                                                     |

### Mode User Exec and Privileged Exec

**Examples** To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user 'manager', use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening on TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server 'example\_host' using an IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

**Example (VRF-lite)** To login to the remote SSH server at 192.168.1.1 on VRF "red", use the command:

```
awplus# ssh vrf red 192.168.1.1
```

**Related commands**

- [crypto key generate userkey](#)
- [crypto key pubkey-chain knownhosts](#)
- [debug ssh client](#)
- [ssh client](#)

**Command changes**

- Version 5.5.3-1.1: added to AR1050V
- Version 5.5.1-1.1: support removed for SSH protocol v1
- Version 5.4.8-2.1: secure mode syntax added for x950, SBx908 GEN2.
- Version 5.4.8-1.2: secure mode syntax added for x220, x930, x550, XS900MX.
- Version 5.4.6-2.1: VRF-lite support added for AR-Series devices.

## ssh client

**Overview** This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the **ssh client** command, and restores the defaults.

This command does not affect the existing SSH sessions.

**Syntax** `ssh client {port <1-65535>|version 2|session-timeout <0-3600>|connect-timeout <1-600>}`  
`no ssh client {port|version|session-timeout|connect-timeout}`

**Syntax (VRF-lite)** `ssh client {port <1-65535>|version 2|session-timeout <0-3600>|connect-timeout <1-600>|vrf <vrf-name>}`  
`no ssh client {port|version|session-timeout|connect-timeout|vrf}`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port            | <p>The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port.</p> <p>Default: 22</p> <hr/> <p>&lt;1-65535&gt; TCP port number.</p>                                                                                                                                                                                                       |
| version         | <p>The SSH version used by the client for SSH sessions.</p> <p>From 5.5.1-1.1 onwards, the SSH client supports only version 2</p>                                                                                                                                                                                                                                                                                          |
| session-timeout | <p>The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout.</p> <p>Default: 0 (session timer remains off)</p> <hr/> <p>&lt;0-3600&gt; Timeout in seconds.</p> |
| connect-timeout | <p>The maximum time period that an SSH session can take to become established. The SSH client terminates the SSH session if this timeout expires and the session is still not established.</p> <p>Default: 30</p> <hr/> <p>&lt;1-600&gt; Timeout in seconds.</p>                                                                                                                                                           |
| vrf <vrf-name>  | <p>The VRF to use for SSH clients.</p> <p>Default: the global VRF.</p>                                                                                                                                                                                                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

**Example (VRF-lite)** To configure SSH clients to use the VRF named 'red', use the command:

```
awplus# ssh client vrf red
```



**Related commands** **show ssh client**  
**ssh**

**Command changes** Version 5.5.3-1.1: added to AR1050V  
Version 5.5.2-1.1: **vrf** parameter added for products that support VRF  
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# ssh client allow-legacy-ssh-rsa

**Overview** Use this command to enable support for the legacy ssh-rsa algorithm on the SSH client. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH client.

**Syntax** ssh client allow-legacy-ssh-rsa  
no ssh client allow-legacy-ssh-rsa

**Default** Disabled

**Mode** Global Configuration

**Example** To enable SSH client support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh client allow-legacy-ssh-rsa
```

**Related commands** [show ssh client](#)  
[ssh client](#)  
[ssh server allow-legacy-ssh-rsa](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V  
Version 5.5.3-0.1: command added

## ssh client vrf

**Overview** Use this command to modify the configured VRF of the SSH client. Use this configuration for any SSH client on the device to connect to remote SSH servers.

Use the **no** variant of this command to restore the configured VRF to the default VRF (global VRF).

**Syntax** `ssh client vrf <vrf-name>`  
`no client vrf`

| Parameter                         | Description                                                             |
|-----------------------------------|-------------------------------------------------------------------------|
| <code>vrf &lt;vrf-name&gt;</code> | The name of the VRF to use for SSH clients. This overrides the default. |

**Default** Global VRF

**Mode** Global Configuration

**Usage notes** Any VRF parameter specified on the SSH client explicitly overrides the default configuration parameters. This also affects the copy commands that utilize SSH such as **copy scp** and **copy sftp**.

This change affects all new user shell sessions. Existing sessions will not be affected.

A user may override this on a per-session basis using the executive mode variant of this command.

**Examples** To configure the VRF named 'management' for SSH clients, use the commands:

```
awplus# configure terminal
awplus(config)# ssh client vrf management
```

To restore to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh client vrf
```

**Related commands** [show ssh client](#)  
[ssh client](#)

**Command changes** Version 5.5.2-2.1: command added

## ssh server

**Overview** Use this command to modify the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

Use the **no** variant of this command to restore the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the **service ssh** command.

**Syntax** `ssh server <1-65535>`  
`ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]  
[max-startups <1-128>]}`  
`no ssh server {[session-timeout] [login-timeout] [max-startups]}`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>       | The TCP port number that the server listens to for incoming SSH sessions.<br><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><br>Default: 0 (session timer remains off).<br><br>Enter a timeout between 0-3600 seconds. |
| login-timeout   | The maximum time period the server waits before disconnecting an unauthenticated client.<br><br>Default: 60<br><br>Enter a timeout between 1- 600 seconds.                                                                                                                                                                                                                 |
| max-startups    | The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection.<br><br>Default: 10<br><br>Enter a number of sessions in the range of 1-128.          |

**Mode** Global Configuration

**Examples** To set the session timer of the SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server session-timeout 600
```

To set the login timeout of the SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting for authentication from the SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups 3
```

To return the limit on the number of waiting connections to the default of 10, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the SSH server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

**Related commands** **show ssh server**  
**ssh server vrf**

**Command changes** Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# ssh server allow-legacy-ssh-rsa

**Overview** Use this command to enable support for the legacy ssh-rsa algorithm on the SSH server. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH server.

**Syntax** ssh server allow-legacy-ssh-rsa  
no ssh server allow-legacy-ssh-rsa

**Default** Disabled

**Mode** Global Configuration

**Example** To enable SSH server support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-legacy-ssh-rsa
```

**Related commands** [show ssh server](#)  
[ssh server](#)

**Command changes** Version 5.5.3-0.1: command added

## ssh server allow-users

**Overview** This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server allow-users <username-pattern> [<hostname-pattern>]`  
`no ssh server allow-users <username-pattern> [<hostname-pattern>]`

| Parameter                             | Description                                                                                                                                                                                                              |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.                                                                                            |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server allows the user to connect only from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters. |

**Mode** Global Configuration

**Examples** To allow the user john to create an SSH session from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john
```

To allow the user john to create an SSH session from a range of IP address (from 192.168.1.1 to 192.168.1.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john 192.168.1.*
```

To allow the user john to create a SSH session from a-company.com domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john *.a-company.com
```

To delete the existing user entry john 192.168.1.\* in the allow list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server allow-users john 192.168.1.*
```

**Related commands** [show running-config ssh](#)  
[show ssh server allow-users](#)  
[ssh server deny-users](#)



# ssh server authentication

**Overview** This command enables RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **ssh server authentication** command to enable password authentication for users. Apply the **publickey** keyword with the **ssh server authentication** command to enable RSA public-key authentication for users.

Use the **no** variant of this command to disable RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **no ssh authentication** command to disable password authentication for users. Apply the required **publickey** keyword with the **no ssh authentication** command to disable RSA public-key authentication for users.

**Syntax** ssh server authentication {password|publickey}  
no ssh server authentication {password|publickey}

| Parameter | Description                                             |
|-----------|---------------------------------------------------------|
| password  | Specifies user password authentication for SSH server.  |
| publickey | Specifies user publickey authentication for SSH server. |

**Default** Both RSA public-key authentication and password authentication are enabled by default.

**Mode** Global Configuration

**Usage** For password authentication to authenticate a user, password authentication for a user must be registered in the local user database or on an external RADIUS server, before using the **ssh server authentication password** command.

For RSA public-key authentication to authenticate a user, a public key must be added for the user, before using the **ssh server authentication publickey** command.

**Examples** To enable password authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication password
```

To enable publickey authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication publickey
```

To disable password authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication password
```

To disable publickey authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication publickey
```

**Related commands** [crypto key pubkey-chain userkey](#)  
[service ssh](#)  
[show ssh server](#)

## ssh server deny-users

**Overview** This command adds a username pattern to the deny list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is rejected.

SSH server also maintains the allow list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

If a hostname pattern is specified, the user is denied from the hosts matching the pattern.

The **no** variant of this command deletes a username pattern from the deny list of the SSH server. To delete an entry from the deny list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server deny-users <username-pattern> [<hostname-pattern>]`  
`no ssh server deny-users <username-pattern> [<hostname-pattern>]`

| Parameter                             | Description                                                                                                                                                                                                                                                                 |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen, full stop and asterisk symbols. An asterisk acts as a wildcard character that matches any string of characters. |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.                                             |

**Mode** Global Configuration

**Examples** To deny the user john to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user john to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user john to access SSH login from b-company.com domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```

To delete the existing user entry john 192.168.2.\* in the deny list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server deny-users john 192.168.2.*
```

**Related commands**

- show running-config ssh**
- show ssh server deny-users**
- ssh server allow-users**

# ssh server 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                                                          |
|-----------|----------------------------------------------------------------------|
|           | Maximum number of SSH authentication attempts the device will allow. |

**Default** 6 attempts

**Mode** Global Configuration

**Usage** By default, users must wait one second after a failed login attempt before trying again. You can increase this gap by using the command [aaa login fail-delay](#).

**Example** To set the maximum number of SSH authentication attempts to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-auth-tries 3
```

**Related commands** [show ssh server](#)

# ssh server resolve-host

**Overview** This command enables resolving an IP address from a host name using a DNS server for client host authentication.

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

**Syntax** `ssh server resolve-hosts`  
`no ssh server resolve-hosts`

**Default** This feature is disabled by default.

**Mode** Global Configuration

**Usage notes** Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. Use the **ip name-server** command to add a DNS server to the list of servers that the device queries.

**Example** To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

**Related commands** **ip name-server**  
**show ssh server**  
**ssh server allow-users**  
**ssh server deny-users**

## ssh server scp

**Overview** This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

**Syntax** ssh server scp  
no ssh server scp

**Mode** Global Configuration

**Examples** To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

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

# ssh server secure-algs

**Overview** Use this command to force the SSH server to only use ciphers, key exchange algorithms and Message Authentication Code (MAC) algorithms that are currently considered best-practice.

This command is the same as using all of the commands **ssh server secure-ciphers**, **ssh server secure-hostkey**, **ssh server secure-mac**, and **ssh server secure-kex**. However, it does not include the optional **exclude-nist-curves** parameter of **ssh server secure-kex**.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of algorithms.

**Syntax** `ssh server secure-algs`  
`no ssh server secure-algs`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of algorithms, use the **show ssh server** command.

**Example** To force the SSH server to use best-practice algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-algs
```

**Related commands** **show ssh server**  
**ssh server**  
**ssh server secure-ciphers**  
**ssh server secure-hostkey**  
**ssh server secure-kex**  
**ssh server secure-mac**

**Command changes** Version 5.5.1-1.1: command added



# ssh server secure-ciphers

**Overview** Use this command to force the SSH server to only negotiate ciphers regarded as current best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of ciphers.

**Syntax** `ssh server secure-ciphers`  
`no ssh server secure-ciphers`

**Default** Not set

**Mode** Global Configuration

**Usage notes** To see the list of ciphers, use the [show ssh server](#) command.

**Example** To configure the SSH server to use best-practice ciphers, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-ciphers
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-kex](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.0-1.1: command added

# ssh server secure-hostkey

**Overview** Use this command to force the SSH server to only use hostkey algorithms that are currently considered best-practice. This excludes NIST curve-based hostkey algorithms.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of hostkey algorithms.

**Syntax** `ssh server secure-hostkey`  
`no ssh server secure-hostkey`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** Using this command may reduce compatibility with older SSH clients.  
To see the list of hostkey algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice hostkey algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-hostkey
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-kex](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.2-2.1: command added

## ssh server secure-kex

**Overview** Use this command to force the SSH server to only use key exchange algorithms that are currently considered best-practice.

For example, using this command stops the device from using the diffie-hellman-group-exchange-sha1 key exchange algorithm.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of key-exchange algorithms.

**Syntax** `ssh server secure-kex [exclude-nist-curves]`  
`no ssh server secure-kex`

| Parameter                        | Description                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <code>exclude-nist-curves</code> | Also exclude all NIST key exchange algorithms.<br><br>Using this parameter may reduce compatibility with older SSH clients. |

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of key exchange algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice key-exchange algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-kex
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.2-2.1: **exclude-nist-curves** parameter added  
Version 5.5.0-2.3: command added

## ssh server secure-mac

**Overview** Use this command to force the SSH server to only use Message Authentication Code (MAC) algorithms that are currently considered best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of MAC algorithms.

**Syntax** `ssh server secure-mac`  
`no ssh server secure-mac`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of MAC algorithms, use the **show ssh server** command.

**Example** To force the SSH server to use best-practice MAC algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-mac
```

**Related commands** **show ssh server**  
**ssh server**  
**ssh server secure-algs**  
**ssh server secure-ciphers**  
**ssh server secure-hostkey**  
**ssh server secure-kex**

**Command changes** Version 5.5.1-1.1: command added

## ssh server sftp

**Overview** This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

**Syntax** ssh server sftp  
no ssh server sftp

**Mode** Global Configuration

**Examples** To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

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

# ssh server tcpforwarding

**Overview** Use this command to enable TCP port forwarding on the SSH server. It is disabled by default, to enhance security.  
Use the **no** variant of this command to disable TCP port forwarding again.

**Syntax** ssh server tcpforwarding  
no ssh server tcpforwarding

**Default** Disabled

**Mode** Global Configuration

**Example** To enable TCP port forwarding, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server tcpforwarding
```

To disable it again, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server tcpforwarding
```

**Related commands** [show ssh server](#)

**Command changes** Version 5.5.2-1.1: command added

# ssh server vrf

**Overview** Use this command to specify a VRF for the SSH server to operate within.  
Use the **no** variant of this command to return the SSH server to the default VRF.

**Syntax** ssh server vrf [*<vrf-name>*]  
no ssh server vrf

| Parameter               | Description                  |
|-------------------------|------------------------------|
| <i>&lt;vrf-name&gt;</i> | The name of the VRF instance |

**Default** The global VRF

**Mode** Global Configuration

**Example** To configure the SSH server to operate within the VRF instance named 'red', use the command:

```
awplus# configure terminal
awplus(config)# ssh server vrf red
```

To return the SSH server to operating within the global VRF instance, use the command:

```
awplus# configure terminal
awplus(config)# no ssh server vrf
```

**Related commands** [show ssh server](#)  
[ssh](#)  
[ssh server](#)

**Command changes** Version 5.5.2-1.1: command added

# undebug ssh client

**Overview** This command applies the functionality of the **no debug ssh client** command.

**Command changes** Version 5.5.3-1.1: added to AR1050V



# undebug ssh server

**Overview** This command applies the functionality of the **no debug ssh server** command.

# 40

## Trigger Commands

- Contents**
- **Introduction** on page 2015
  - **active (trigger)** on page 2016
  - **day** on page 2017
  - **debug trigger** on page 2019
  - **description (trigger)** on page 2020
  - **repeat** on page 2021
  - **script** on page 2023
  - **show debugging trigger** on page 2025
  - **show running-config trigger** on page 2026
  - **show trigger** on page 2027
  - **test** on page 2032
  - **time (trigger)** on page 2033
  - **trap** on page 2035
  - **trigger** on page 2036
  - **trigger activate** on page 2037
  - **type atmf guest** on page 2038
  - **type atmf node** on page 2039
  - **type cpu** on page 2042
  - **type env-sensor** on page 2044
  - **type interface** on page 2047
  - **type linkmon-probe** on page 2048
  - **type log** on page 2050
  - **type memory** on page 2051
  - **type periodic** on page 2052
  - **type ping-poll** on page 2053
  - **type reboot** on page 2054
  - **type time** on page 2055
  - **undebug trigger** on page 2056

# 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](#).

# active (trigger)

**Overview** This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

**Syntax** active  
no active

**Default** Active, which means that triggers are enabled by default

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to activate it.  
For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

**Related commands** [show trigger](#)  
[trigger](#)  
[trigger activate](#)

# day

**Overview** This command specifies the days or date that the trigger can activate on. You can specify one of:

- A specific date
- A specific day of the week
- A list of days of the week
- A day of any month of any year
- A day of a specific month in any year
- Every day

By default, the trigger can activate on any day.

**Syntax** day every-day  
day <1-31>  
day <1-31> <month>  
day <1-31> <month> <year>  
day <weekday>

| Parameter | Description                                                                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| every-day | Sets the trigger so that it can activate on any day.                                                                                                                                                                                                                                   |
| <1-31>    | Day of the month the trigger is permitted to activate on.                                                                                                                                                                                                                              |
| <month>   | Sets the month that the trigger is permitted to activate on. Valid keywords are: <b>january</b> , <b>february</b> , <b>march</b> , <b>april</b> , <b>may</b> , <b>june</b> , <b>july</b> , <b>august</b> , <b>september</b> , <b>october</b> , <b>november</b> , and <b>december</b> . |
| <year>    | Sets the year that the trigger is permitted to activate in, between 2000 and 2035.                                                                                                                                                                                                     |
| <weekday> | Sets the days of the week that the trigger can activate on. You can specify one or more week days in a space separated list. Valid keywords are: <b>monday</b> , <b>tuesday</b> , <b>wednesday</b> , <b>thursday</b> , <b>friday</b> , <b>saturday</b> , and <b>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** Privileged 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** [show trigger](#)  
**commands** [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** The following shows typical output.

## Example output from the show debugging trigger command

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
 Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
 Trigger debugging is off
```

**Related commands** **debug trigger**

# show running-config trigger

**Overview** This command displays the current running configuration of the trigger utility.

**Syntax** show running-config trigger

**Mode** Privileged Exec

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

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

**Output** The following shows typical output.

**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
```

### Example output from show trigger

```
awplus#show trigger
```

| TR# | Type & Details    | Name                 | Ac | Te | Repeat     | #Scr | Days/Date |
|-----|-------------------|----------------------|----|----|------------|------|-----------|
| 001 | CPU (80% any)     | Busy CPU             | Y  | N  | 5          | 1    | smtwtfs   |
| 005 | Periodic (30 min) | Regular status check | Y  | N  | Continuous | 1    | -mtwtf-   |
| 007 | Memory (85% up)   | High mem usage       | Y  | N  | 8          | 1    | smtwtfs   |
| 011 | Time (00:01)      | Weekend access       | Y  | N  | Continuous | 1    | -----s    |
| 013 | Reboot            |                      | Y  | N  | Continuous | 2    | smtwtfs   |
| 019 | Ping-poll (5 up)  | Connection to svr1   | Y  | N  | Continuous | 1    | smtwtfs   |

### 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 <b>description (trigger)</b> command.                                                                                                                           |
| Ac             | Whether the trigger is active (Y), or inactive (N).                                                                                                                                                                 |
| 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 &lt;1-250&gt;</b> 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
```

### Example output from show trigger for a specific trigger

```
awplus#show trigger 1
```

| Trigger Configuration Details |                                 |
|-------------------------------|---------------------------------|
| Trigger .....                 | 1                               |
| Name .....                    | display cpu usage when pass 80% |
| Type and details .....        | CPU (80% up)                    |
| Days .....                    | smtwtfs                         |



```
Active Yes
Test No
Trap Yes
Repeat Continuous
Modified Fri Feb 3 17:18:44 2017
Number of activations 0
Last activation not activated
Number of scripts 1
1. shocpu.scp
2.
3.
4.
5.

```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

### 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 smtwtfss
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 smtwtfss
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.

```

### Parameters in the output of show trigger full and show trigger for a specific trigger

| Parameter | Description            |
|-----------|------------------------|
| Trigger   | The ID of the trigger. |

| Parameter             | Description                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                       |
| 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
```

### Example output from show trigger counter

```
awplus# show trigger counter
Trigger Module Counters

Trigger activations 4
Last trigger activated 55
Time triggers activated today 0
Periodic triggers activated today 0
Interface triggers activated today 1
CPU triggers activated today 2
Memory triggers activated today 1
Reboot triggers activated today 0
Ping-poll triggers activated today 0
USB event triggers activated today 0
Stack master fail triggers activated today 0
```

|                                       |   |
|---------------------------------------|---|
| Stack member triggers activated today | 0 |
| Stack link triggers activated today   | 0 |
| ATMF node triggers activated today    | 0 |
| ATMF guest triggers activated today   | 0 |
| Log triggers activated today          | 0 |
| -----                                 |   |

- Related commands

active (trigger)

debug trigger

script

trigger

trigger activate

# test

**Overview** This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates, the scripts associated with the trigger will be run, as normal.

**Syntax** test  
no test

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

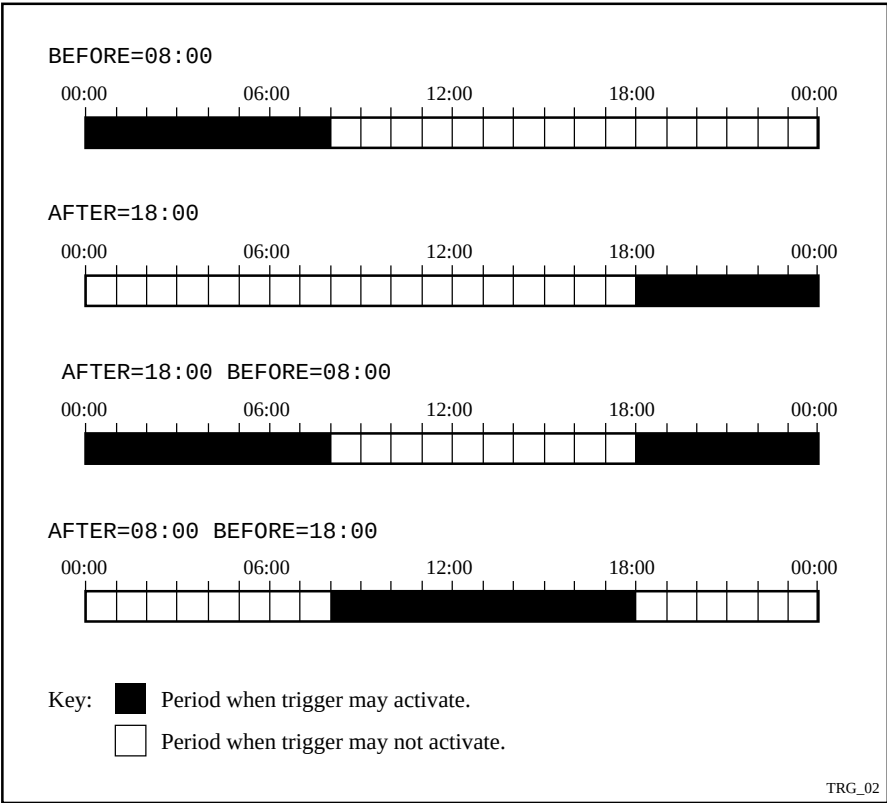
```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

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

# time (trigger)

**Overview** This command specifies the time of day when the trigger is permitted to activate. The **after** parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from "after" to "before" is defined, during which the trigger may activate. This command is not applicable to time triggers ( **type time** ).

The following figure illustrates how the **before** and **after** parameters operate.



**Syntax** time {[after <hh:mm:ss>] [before <hh:mm:ss>]}

| Parameter        | Description                                                 |
|------------------|-------------------------------------------------------------|
| after<hh:mm:ss>  | The earliest time of day when the trigger may be activated. |
| before<hh:mm:ss> | The latest time of day when the trigger may be activated.   |

**Mode** Trigger Configuration

**Usage notes** For example trigger configurations that use the **time (trigger)** command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To allow trigger 63 to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger 64 to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger 65 to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

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

# trap

**Overview** This command enables the specified trigger to send SNMP traps.

Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

**Syntax** trap  
no trap

**Default** SNMP traps are enabled by default for all defined triggers.

**Mode** Trigger Configuration

**Usage notes** You must configure SNMP before using traps with triggers. For more information, see:

- [Support for Allied Telesis Enterprise\\_MIBs\\_in AlliedWare Plus](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration\\_Guide](#).
- the [SNMP Commands](#) chapter.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the [Support for Allied Telesis Enterprise\\_MIBs\\_in AlliedWare Plus](#) for further information about the relevant SNMP MIB.

**Examples** To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

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

# trigger

**Overview** This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

**Syntax** trigger <1-250>  
no trigger <1-250>

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Global Configuration

**Examples** To enter trigger configuration mode for trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
```

To completely remove all configuration associated with trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# no trigger 12
```

**Related commands** [show trigger](#)  
[trigger activate](#)



# trigger activate

**Overview** This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

**Syntax** trigger activate <1-250>

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Privileged Exec

**Usage notes** This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it has been configured as inactive by using the command **no active**. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

**Example** To manually activate trigger 12 use the command:

```
awplus# trigger activate 12
```

**Related commands** [active \(trigger\)](#)  
[show trigger](#)  
[trigger](#)

# type atmf guest

**Overview** This command configures a trigger to activate when an AMF guest node joins or leaves.

**Syntax** type atmf guest {join|leave}

| Parameter | Description            |
|-----------|------------------------|
| join      | AMF guest node joins.  |
| leave     | AMF guest node leaves. |

**Mode** Trigger Configuration

**Example** To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

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

**Command changes** Version 5.5.1-1.1: command added

## type atmf node

**Overview** This command configures a trigger to activate when an AMF node joins or leaves.

**Syntax** type atmf node {join|leave}

| Parameter | Description      |
|-----------|------------------|
| join      | AMF node joins.  |
| leave     | AMF node leaves. |

**Mode** Trigger Configuration

**Example 1** To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

**Example 2** The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=====
node1:
=====

TR# Type & Details Description Ac Te Tr Repeat #Scr Days/Date

001 Periodic (2 min) Periodic Status Chk Y N Y Continuous 1 smtwtfS
005 ATMF node (leave) E-mail on ATMF Exit Y N Y Continuous 1 smtwtfS

=====
Node2, Node3,
=====

TR# Type & Details Description Ac Te Tr Repeat #Scr Days/Date

005 ATMF node (leave) E-mail on ATMF Exit Y N Y Continuous 1 smtwtfS

```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
=====
Node1:
```

```
=====

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

=====
Node2, Node3:
=====

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

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

# 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** [show trigger](#)  
**commands** [trigger](#)

## type env-sensor

**Overview** Use this command to create a trigger that will run a script when the device's environment sensors detect an event. Environment sensors are shown in the output of the command **show system environment**, and include things like device temperature, power settings and voltage.

Depending on the device and sensor, you can create a trigger to run when:

- the sensor's state changes, for example when a loss of power is detected for a power supply, or when power is restored, or both.
- the sensor's reading crosses a high or low threshold, for example when the device temperature becomes too high, or returns to normal, or both.

**Syntax when  
a sensor  
changes  
state**

```
type env-sensor resource <resource-id> sensor <sensor-id> state {true|false|any}
```

| Parameter                 | Description                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| resource<br><resource-id> | The 'Resource ID' for the device, as shown in output of the command <b>show system environment</b> .                           |
| sensor<br><sensor-id>     | The 'ID' for the sensor, as shown in output of the command <b>show system environment</b> .                                    |
| state true                | The trigger will activate if this sensor reading changes to 'Yes' or 'Open' in the output of <b>show system environment</b> .  |
| state false               | The trigger will activate if this sensor reading changes to 'No' or 'Closed' in the output of <b>show system environment</b> . |
| state any                 | The trigger will activate if this sensor reading changes to any of 'Yes', 'Open', 'No', or 'Closed'.                           |



**Syntax when  
a sensor  
crosses a  
threshold**

type env-sensor resource <resource-id> sensor <sensor-id> {low-limit|high-limit} {exceeded|cleared|any}

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| resource<br><resource-id> | The 'Resource ID' for the device, as shown in output of the command <b>show system environment</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| sensor<br><sensor-id>     | The 'ID' for the sensor, as shown in output of the command <b>show system environment</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| low-limit                 | The trigger will activate when the sensor reading falls below the 'Low Limit' alarm threshold shown in <b>show system environment</b> , or returns to an acceptable value after being too low, or both. The alarm threshold values are pre-defined within the device and cannot be changed.                                                                                                                                                                                                                                                     |
| high-limit                | The trigger will activate when the sensor reading rises above the 'High Limit' alarm threshold shown in <b>show system environment</b> , or returns to an acceptable value after being too high, or both. The alarm threshold values are pre-defined within the device and cannot be changed.                                                                                                                                                                                                                                                   |
| exceeded                  | If you chose low-limit, the trigger will trigger if the sensor's reading falls below the low limit.<br><br>If you chose high-limit, the trigger will trigger if the sensor's reading goes above the high limit.                                                                                                                                                                                                                                                                                                                                 |
| cleared                   | If you chose low-limit, the trigger will trigger if the sensor's reading rises to above the low limit again.<br><br>If you chose high-limit, the trigger will trigger if the sensor's reading falls below the high limit again.<br><br>Some temperature sensors include a hysteresis value and will not clear until the temperature has changed significantly. For example, if a sensor has a high alarm threshold of 75 degrees Celsius, the hysteresis value may mean that the alarm clears when the temperature falls to 63 degrees Celsius. |
| any                       | The trigger will trigger if the low or high limit is either exceeded or cleared.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Mode** Trigger Configuration

**Example** To configure trigger 1, which will activate when the internal temperature becomes too high or drops to a low-enough value after being too high, use the following commands. In this example, the monitored temperature has a resource ID of 4 and a sensor ID of 6:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type env-sensor resource 4 sensor 6
high-limit any
```

**Related commands** **show system environment**  
**show trigger**  
**trigger**

**Command changes** Version 5.5.2-1.1: command added

# type interface

**Overview** This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

**Syntax** type interface <interface> {up|down|any}

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <interface> | Interface name.                                       |
| up          | Activate when interface becomes operational.          |
| down        | Activate when the interface closes.                   |
| any         | Activate when any interface link status event occurs. |

**Mode** Trigger Configuration

**Example** To configure trigger 19 to be an interface trigger that activates when eth1 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface eth1 up
```

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

## type linkmon-probe

**Overview** Use this command to create a trigger that will run a script when a Link Health Monitoring probe reports that a link becomes “good”, “bad”, or “unreachable”.

**Syntax** type linkmon-probe <probename> <profilename> {good|bad|unreachable|any}

| Parameter     | Description                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <probename>   | The name of the Link Health Monitoring probe that will be used for executing the trigger.                                                                    |
| <profilename> | The name of the Link Health Monitoring performance profile that will be used for determine if the Link Health Monitoring probe is good, bad, or unreachable. |
| good          | If the Link Health Monitoring probe becomes 'good' according to the Link Health Monitoring performance profile then the trigger will be executed.            |
| bad           | If the Link Health Monitoring probe goes 'bad' according to the Link Health Monitoring performance profile then the trigger will be executed.                |
| unreachable   | If the Link Health Monitoring probe becomes 'unreachable' according to the Link Health Monitoring performance profile then the trigger will be executed.     |
| any           | If the Link Health Monitoring probe changes state according to the Link Health Monitoring performance profile then the trigger will be executed.             |

**Mode** Trigger Configuration

**Example** When the Link Health Monitoring probes sent to the “test-probe” destination no longer meet the performance profile “test-profile” the link will be deemed “bad”. To create a trigger that will run a script when a Link Health Monitoring probe is deemed “bad”, use the following commands:

```
awplus(config)# trigger 1
awplus(config-trigger)# script 1 link-bad.scp
awplus(config-trigger)# type linkmon-probe test-probe test-profile bad
```

To create a trigger that will run a script when the link is deemed “good” again, use the following commands:

```
awplus(config)# trigger 2
awplus(config-trigger)# script 1 link-good.scp
awplus(config-trigger)# type linkmon-probe test-probe test-profile good
```

**Related** **trigger**  
**commands**

**Command** Version 5.4.8-1.1: command added  
**changes**

## type log

**Overview** Use this command to configure a trigger to activate based on the content of log messages matching a string or regular expression.

**Syntax** type log <log-message-string>

| Parameter            | Description                                                                              |
|----------------------|------------------------------------------------------------------------------------------|
| <log-message-string> | A string or a regular expression (PCRE) to match a log message or part of a log message. |

**Default** There is no type or log message string set by default.

**Mode** Trigger Configuration

**Usage notes** Log type triggers fully support regular expressions using PCRE (Perl-Compatible Regular Expression) syntax.

Only log messages of severity level notice or higher can activate a trigger.

Note that any command executed by the script will generate a log message with level notice, and will include '[SCRIPT]' before the command string. Therefore, if something in the script matches the configured log message trigger string, it will retrigger indefinitely.

**Example** To configure trigger 6 to activate when a log message of level notice or higher indicates that any port has 'failed', use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# type log port.+ failed
```

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

**Command changes** Version 5.4.7-2.1: command added

## type memory

**Overview** This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

**Syntax** type memory <1-100> [up|down|any]

| Parameter | Description                                                                |
|-----------|----------------------------------------------------------------------------|
| <1-100>   | The percentage of memory usage at which to trigger.                        |
| up        | Activate when memory usage exceeds the specified level.                    |
| down      | Activate when memory usage drops below the specified level.                |
| any       | Activate when memory usage passes the specified level in either direction. |

**Mode** Trigger Configuration

**Examples** To configure trigger 12 to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger 40 to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65

or

awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

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

# type periodic

**Overview** This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

**Syntax** type periodic <1-1440>

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <1-1440>  | The number of minutes between activations. |

**Mode** Trigger Configuration

**Usage notes** A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

|                                                                         |
|-------------------------------------------------------------------------|
| % Cannot configure more than 10 triggers with the type time or periodic |
|-------------------------------------------------------------------------|

For an example trigger configuration that uses the **type periodic** command, see "See Daily Statistics" in the [Triggers\\_Feature Overview and Configuration Guide](#).

**Example** To configure trigger 44 to activate periodically at 10 minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

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



# type ping-poll

**Overview** This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

**Syntax** type ping-poll <1-100> {up|down}

| Parameter | Description                                                                     |
|-----------|---------------------------------------------------------------------------------|
| <1-100>   | The ping poll ID.                                                               |
| up        | The trigger activates when ping polling detects that the target is reachable.   |
| down      | The trigger activates when ping polling detects that the target is unreachable. |

**Mode** Trigger Configuration

**Example** To configure trigger 106 to activate when ping poll 12 detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

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

# type reboot

**Overview** This command configures a trigger that activates when your device is rebooted.

**Syntax** type reboot

**Mode** Trigger Configuration

**Example** To configure trigger 32 to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

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

# type time

**Overview** This command configures a trigger that activates at a specified time of day.

**Syntax** type time <hh:mm>

| Parameter | Description                       |
|-----------|-----------------------------------|
| <hh:mm>   | The time to activate the trigger. |

**Mode** Trigger Configuration

**Usage** A combined limit of 10 triggers of the type time and type periodic can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or periodic
```

**Example** To configure trigger 86 to activate at 15:53, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type time 15:53
```

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

# undebug trigger

**Overview** This command applies the functionality of the **no debug trigger** command.

# 41

## Ping-Polling Commands

- Contents**
- **Introduction** on page 2058
  - **active (ping-polling)** on page 2059
  - **clear ping-poll** on page 2060
  - **critical-interval** on page 2061
  - **debug ping-poll** on page 2062
  - **description (ping-polling)** on page 2063
  - **fail-count** on page 2064
  - **ip (ping-polling)** on page 2066
  - **length (ping-poll data)** on page 2067
  - **normal-interval** on page 2068
  - **ping-poll** on page 2069
  - **sample-size** on page 2070
  - **show counter ping-poll** on page 2072
  - **show ping-poll** on page 2075
  - **source-ip** on page 2079
  - **timeout (ping polling)** on page 2081
  - **up-count** on page 2082
  - **undebug ping-poll** on page 2083

# 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](#).

**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                                                                          |

## active (ping-polling)

**Overview** This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the **ip (ping-polling)** command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

**Syntax** active  
no active

**Mode** Ping-Polling Configuration

**Examples** To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

**Related commands** **debug ping-poll**  
**ip (ping-polling)**  
**ping-poll**  
**show ping-poll**

# clear ping-poll

**Overview** This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the **critical-interval** command. The device status changes to reachable once the device responses have reached the **up-count**.

**Syntax** `clear ping-poll {<1-100>|all}`

| Parameter | Description                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable. |
| all       | Clears the counters and changes the device status of all polling instances.                                                                        |

**Mode** Privileged Exec

**Examples** To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

**Related commands** **active (ping-polling)**  
**ping-poll**  
**show ping-poll**



# critical-interval

**Overview** This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the **normal-interval** command.

The **no** variant of this command sets the critical interval to the default of one second.

**Syntax** critical-interval <1-65536>  
no critical-interval

| Parameter | Description                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------|
| <1-65536> | Time in seconds between pings, when the device has failed to a ping, or the device is unreachable. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

**Related commands**

- fail-count**
- normal-interval**
- sample-size**
- show ping-poll**
- timeout (ping polling)**
- up-count**

# debug ping-poll

**Overview** This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

**Syntax** debug ping-poll <1-100>  
no debug ping-poll {<1-100>|all}

| Parameter | Description                       |
|-----------|-----------------------------------|
| <1-100>   | A unique ping poll ID number.     |
| all       | Turn off all ping-poll debugging. |

**Mode** Privileged Exec

**Examples** To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

**Related commands**

- [active \(ping-polling\)](#)
- [clear ping-poll](#)
- [ping-poll](#)
- [show ping-poll](#)
- [undebug ping-poll](#)

# description (ping-polling)

**Overview** This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;description&gt;</code> | The description of the target. Valid characters are any printable character and spaces. There is no maximum character length. |

**Mode** Ping-Polling Configuration

**Examples** To add the text "Primary Gateway" to describe the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# description Primary Gateway
```

To delete the description set for the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no description
```

**Related commands** [ping-poll](#)  
[show ping-poll](#)

# fail-count

**Overview** This command specifies the number of pings that must be unanswered, within the total number of pings specified by the **sample-size** command, for the ping-polling instance to consider the device unreachable.

If the number set by the **sample-size** command and the **fail-count** commands are the same, then the unanswered pings must be consecutive. If the number set by the **sample-size** command is greater than the number set by the **fail-count** command, then a device that does not always reply to pings may be declared unreachable.

The **no** variant of this command resets the fail count to the default.

**Syntax** fail-count <1-100>  
no fail-count

| Parameter | Description                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To specify the number of pings that must fail within the sample size to determine that a device is unreachable for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# fail-count 5
```

To reset the fail-count to its default of 5 for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no fail-count
```

**Related commands**

- critical-interval**
- normal-interval**
- ping-poll**
- sample-size**
- show ping-poll**
- timeout (ping polling)**
- up-count**

# ip (ping-polling)

**Overview** This command specifies the IPv4 address of the device you are polling.

**Syntax** `ip {<ip-address>|<ipv6-address>}`

| Parameter                         | Description                                        |
|-----------------------------------|----------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | An IPv4 address in dotted decimal notation A.B.C.D |
| <code>&lt;ipv6-address&gt;</code> | An IPv6 address in hexadecimal notation X:X::X:X   |

**Mode** Ping-Polling Configuration

**Examples** To set ping-poll instance 5 to poll the device with the IP address 192.168.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 5
awplus(config-ping-poll)# ip 192.168.0.1
```

To set ping-poll instance 10 to poll the device with the IPv6 address 2001:db8::, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 10
awplus(config-ping-poll)# ip 2001:db8::
```

**Related commands**

- [ping-poll](#)
- [source-ip](#)
- [show ping-poll](#)

## length (ping-poll data)

**Overview** This command specifies the number of data bytes to include in the data portion of the ping packet. This allows you to set the ping packets to a larger size if you find that larger packet types in your network are not reaching the polled device, while smaller packets are getting through. This encourages the polling instance to change the device's status to unreachable when the network is dropping packets of the size you are interested in.

The **no** variant of this command resets the data bytes to the default of 32 bytes.

**Syntax** length <4-1500>  
no length

| Parameter | Description                                                                 |
|-----------|-----------------------------------------------------------------------------|
| <4-1500>  | The number of data bytes to include in the data portion of the ping packet. |

**Default** The default is 32.

**Mode** Ping-Polling Configuration

**Examples** To specify that ping-poll instance 12 sends ping packet with a data portion of 56 bytes, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length 56
```

To reset the number of data bytes in the ping packet to the default of 32 bytes for ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length
```

**Related commands** [ping-poll](#)  
[show ping-poll](#)

# normal-interval

**Overview** This command specifies the time period between pings when the device is reachable.

The **no** variant of this command resets the time period to the default of 30 seconds.

**Syntax** normal-interval <1-65536>  
no normal-interval

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| <1-65536> | Time in seconds between pings when the target is reachable. |

**Default** The default is 30 seconds.

**Mode** Ping-Polling Configuration

**Examples** To specify a time period of 60 seconds between pings when the device is reachable for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# normal-interval 60
```

To reset the interval to the default of 30 seconds for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no normal-interval
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)



# ping-poll

**Overview** This command enters the ping-poll configuration mode. If a ping-poll exists with the specified number, then this command enters its configuration mode. If no ping poll exists with the specified number, then this command creates a new ping poll with this ID number.

To configure a ping-poll, create a ping poll using this command, and use the **ip (ping-polling)** command to specify the device you want the polling instance to poll. It is not necessary to specify any further commands unless you want to change a command's default.

The **no** variant of this command deletes the specified ping poll.

**Syntax** ping-poll <1-100>  
no ping-poll <1-100>

| Parameter | Description                   |
|-----------|-------------------------------|
| <1-100>   | A unique ping poll ID number. |

**Mode** Global Configuration

**Examples** To create ping-poll instance 3 and enter ping-poll configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 3
awplus(config-ping-poll)#
```

To delete ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# no ping-poll 3
```

**Related commands**

- active (ping-polling)**
- clear ping-poll**
- debug ping-poll**
- description (ping-polling)**
- ip (ping-polling)**
- length (ping-poll data)**
- show ping-poll**
- source-ip**

## sample-size

**Overview** This command sets the total number of pings that the polling instance inspects when determining whether a device is unreachable. If the number of pings specified by the **fail-count** command go unanswered within the inspected sample, then the device is declared unreachable.

If the numbers set in this command and **fail-count** command are the same, the unanswered pings must be consecutive. If the number set by this command is greater than that set with the **fail-count** command, a device that does not always reply to pings may be declared unreachable.

You cannot set this command's value lower than the **fail-count** value.

The polling instance uses the number of pings specified by the **up-count** command to determine when a device is reachable.

The **no** variant of this command resets this command to the default.

**Syntax** sample-size <1-100>  
no sample size

| Parameter | Description                                             |
|-----------|---------------------------------------------------------|
| <1-100>   | Number of pings that determines critical and up counts. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```

**Related**  
**commands**

- critical-interval**
- fail-count**
- normal-interval**
- ping-poll**
- show ping-poll**
- timeout (ping polling)**
- up-count**

# show counter ping-poll

**Overview** This command displays the counters for ping polling.

**Syntax** show counter ping-poll [<1-100>]

| Parameter | Description                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | A unique ping poll ID number. This displays the counters for the specified ping poll only. If you do not specify a ping poll, then this command displays counters for all ping polls. |

**Mode** User Exec and Privileged Exec

**Example** To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

**Output** The following shows typical output.

**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
```

**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><br>This error can occur when your device does not have a route to the destination. |
| CurrentUpCount       | The current number of sequential ping replies.                                                                                                                   |

| Parameter        | Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------|
| CurrentFailCount | The number of ping requests that have not received a ping reply in the current sample-size window. |
| UpStateEntered   | Number of times the target device has entered the Up state.                                        |
| DownStateEntered | Number of times the target device has entered the Down state.                                      |

**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

**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
```

**Output** The following shows typical output.

### 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 |

### 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 <b>ping-poll</b> command.                                                |
| Enabled     | Whether the polling instance is enabled or disabled.                                                                                                            |
| 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 <b>ip (ping-polling)</b> command.                                                                             |

### 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

```

### Parameters in output of the show ping-poll command

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|--------------------------|------|----------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Description            | Optional description set for the polling instance with the <b>description (ping-polling)</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |
| Destination IP address | The IP address of the polled device, set with the <b>ip (ping-polling)</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |
| Status                 | <p>The current status of the device being polled:</p> <table> <tr> <td>Up</td><td>The device is reachable.</td></tr> <tr> <td>Down</td><td>The device is unreachable.</td></tr> <tr> <td>Critical Up</td><td>The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.</td></tr> <tr> <td>Critical Down</td><td>The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.</td></tr> </table> | 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. |
| 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 <b>active (ping-polling)</b> and <b>active (ping-polling)</b> commands enable and disable a polling instance.                                                                                                                                                                                                                                                                                                                                                                                  |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |
| Source IP address      | The source IP address sent in the ping packets. This is set using the <b>source-ip</b> 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 <b>critical-interval</b> command.                                                                                                                                                                                                                                                                                                                                            |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |
| Normal interval        | The time period between pings when the device is reachable. This is set with the <b>normal-interval</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                        |    |                          |      |                            |             |                                                                                                                                       |               |                                                                                                                                          |

| Parameter   | Description                                                                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fail count  | The number of pings that must be unanswered, within the total number of pings specified by the <b>sample-size</b> command, for the polling instance to consider the device unreachable. This is set using the <b>fail-count</b> 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 <b>up-count</b> 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 <b>sample-size</b> command.                                                                         |
| Length      | The number of data bytes to include in the data portion of the ping packet. This is set using the <b>length (ping-poll data)</b> command.                                                                                                |
| Timeout     | The time in seconds that the polling instance waits for a response to a ping packet. This is set using the <b>timeout (ping polling)</b> command.                                                                                        |
| Debugging   | Indicates whether ping polling debugging is <b>Enabled</b> or <b>Disabled</b> .<br><br>This is set using the <b>debug ping-poll</b> command.                                                                                             |

**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
```

|                         |                                   |
|-------------------------|-----------------------------------|
| <b>Related commands</b> | <b>description (ping-polling)</b> |
|                         | <b>ip (ping-polling)</b>          |
|                         | <b>length (ping-poll data)</b>    |
|                         | <b>ping-poll</b>                  |
|                         | <b>show ping-poll</b>             |

# timeout (ping polling)

**Overview** This command specifies the time in seconds that the polling instance waits for a response to a ping packet. You may find a higher time-out useful in networks where ping packets have a low priority.

The **no** variant of this command resets the set time out to the default of one second.

**Syntax** `timeout <1-30>`  
`no timeout`

| Parameter | Description                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------|
| <1-30>    | Length of time, in seconds, that the polling instance waits for a response from the polled device. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To specify the timeout as 5 seconds for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# timeout 5
```

To reset the timeout to its default of 1 second for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no timeout
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [up-count](#)

# up-count

**Overview** This command sets the number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again.

The **no** variant of this command resets the up count to the default of 30.

**Syntax** up-count <1-100>  
no up-count

| Parameter | Description                                                                      |
|-----------|----------------------------------------------------------------------------------|
| <1-100>   | Number of replied pings before an unreachable device is classified as reachable. |

**Default** The default is 30.

**Mode** Ping-Polling Configuration

**Examples** To set the upcount to 5 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# up-count 5
```

To reset the upcount to the default value of 30 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no up-count
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)

# undebug ping-poll

**Overview** This command applies the functionality of the no **debug ping-poll**.

# **Part 6: Firewall and Network Address Translation (NAT)**



# 42

## Firewall Commands

- Contents**
- **Introduction** on page 2086
  - **clear firewall connections** on page 2087
  - **connection-limit (firewall)** on page 2088
  - **connection-log events** on page 2090
  - **debug firewall** on page 2091
  - **firewall** on page 2092
  - **geoip update-interval** on page 2093
  - **ip subnet dynamic geoip** on page 2094
  - **ipv6 subnet dynamic geoip** on page 2095
  - **ip tcp timeout established** on page 2096
  - **move rule (firewall)** on page 2097
  - **protect (firewall)** on page 2098
  - **rule (firewall)** on page 2099
  - **show connection-log events** on page 2103
  - **show firewall** on page 2104
  - **show firewall connections** on page 2105
  - **show firewall connections limits** on page 2106
  - **show firewall connections limits config-check** on page 2107
  - **show firewall rule** on page 2108
  - **show firewall rule config-check** on page 2110
  - **show debugging firewall** on page 2111
  - **show running-config firewall** on page 2112

# 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.

## Firewall commands and applicable modes

| Mode                   | Command                                         |
|------------------------|-------------------------------------------------|
| Privileged Exec        | <a href="#">clear firewall connections</a>      |
|                        | <a href="#">debug firewall</a>                  |
|                        | <a href="#">show debugging firewall</a>         |
|                        | <a href="#">show firewall</a>                   |
|                        | <a href="#">show firewall connections</a>       |
|                        | <a href="#">show firewall rule</a>              |
|                        | <a href="#">show firewall rule config-check</a> |
|                        | <a href="#">show running-config firewall</a>    |
| Global Configuration   | <a href="#">firewall</a>                        |
| Firewall Configuration | <a href="#">protect (firewall)</a>              |
|                        | <a href="#">rule (firewall)</a>                 |
|                        | <a href="#">move rule (firewall)</a>            |

# 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. The limit imposed by a connection-limit rule applies to the sum of TCP and UDP flows that match the rule.

You can use the tab key to auto-complete entity names.

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** **show firewall connections**  
**commands** **show firewall connections limits**

**Command** Version 5.5.0-1.1: Firewall session limiting rules apply to UDP connections,  
**changes** where previously the limiting rules only applied to TCP connections.

# 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.

# 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](#)

# 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)**.
- Create, move, or delete rules for the firewall, see the **rule (firewall)** and the **move rule (firewall)**.

**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**



# geoip update-interval

**Overview** Use this command to configure how often the GeoIP resource will be automatically downloaded from the Allied Telesis update server.

Use the **no** variant of this command to return to the default value of 24 hours.

**Syntax** `geoip update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`  
`no geoip update-interval`

| Parameter           | Description                                     |
|---------------------|-------------------------------------------------|
| minutes <10-525600> | Update interval from 10 through 52600 minutes.  |
| hours <1-8760>      | Update interval from 1 hour through 8760 hours. |
| days <1-365>        | Update interval from 1 day through 365 days.    |
| weeks <1-52>        | Update interval from 1 week through 52 weeks.   |
| never               | Never update the GeoIP resource.                |

**Default** 24 hours.

**Mode** Global Configuration

**Example** To configure the update interval of the GeoIP resource to 4 hours, use the commands:

```
awplus# configure terminal
awplus(config)# geoip update-interval hours 4
```

To return the update interval of the GeoIP resource to the default of 24 hours, use the commands:

```
awplus# configure terminal
awplus(config)# no geoip update-interval
```

**Related commands** [ipv6 subnet dynamic geoip](#)  
[ip subnet dynamic geoip](#)

**Command changes** Version 5.5.4-2.3: command added

# ip subnet dynamic geoip

**Overview** Use this command to create a network entity that will dynamically update with subnets from the GeoIP resource. This entity can then be used, for example, in Firewall rules to block traffic from a particular country.

Use the **no** variant of this command to remove a network entity that blocks traffic from a particular country.

**Syntax** `ip subnet dynamic geoip <country-code>`  
`no ip subnet dynamic geoip <country-code>`

| Parameter      | Description           |
|----------------|-----------------------|
| <country-code> | ISO 3166 Country_Code |

**Mode** Network Configuration

**Usage notes** The GeoIP resource will be downloaded from the Allied Telesis updates server automatically. GeoIP networks are based on country of registration, not location, therefore the **accuracy of the data cannot be guaranteed**.

**Example** To configure an entity to block traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# ip subnet dynamic geoip RU
```

To remove the entity that blocks traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# no ip subnet dynamic geoip RU
```

**Related commands** [ipv6 subnet dynamic geoip](#)  
[geoip update-interval](#)

**Command changes** Version 5.5.4-2.2: command added

# ipv6 subnet dynamic geoip

**Overview** Use this command to create a network entity that will dynamically update with subnets from the GeoIP resource. This entity can then be used, for example, in Firewall rules to block traffic from a particular country.

Use the **no** variant of this command to remove a network entity that blocks traffic from a particular country.

**Syntax** `ipv6 subnet dynamic geoip <country-code>`  
`no ipv6 subnet dynamic geoip <country-code>`

| Parameter      | Description                  |
|----------------|------------------------------|
| <country-code> | <b>ISO 3166 Country_Code</b> |

**Mode** Network Configuration

**Usage notes** The GeoIP resource will be downloaded from the Allied Telesis updates server automatically. GeoIP networks are based on country of registration, not location, therefore the **accuracy of the data cannot be guaranteed**.

**Example** To configure an entity to block traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# ipv6 subnet dynamic geoip RU
```

To remove the entity that blocks traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# no ipv6 subnet dynamic geoip RU
```

**Related commands** [ip subnet dynamic geoip](#)  
[geoip update-interval](#)

**Command changes** Version 5.5.4-2.2: 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                                                                |
|--------------|----------------------------------------------------------------------------|
| <1-31536000> | 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                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| move rule<br><1-65535> | Move the ID of a given rule. The rule ID of the given rule must exist.<br><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. |
| to <1-65535>           | 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 \(firewall\)](#) 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                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>          | Rule ID is an integer in the range <1-65535>. 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.                                                                                                 |
| <application-name> | Application name. You can either specify an application name or use the word <b>any</b> , which stands for all applications. For more information about applications, see <a href="#">Application and Entity Commands</a> .<br><br>You can use the tab key to auto-complete application names.  |
| <source-entity>    | Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces. For more information about entities, see <a href="#">Application and Entity Commands</a> .                                                                                                         |



| Parameter                         | Description                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                                                               |
| <i>&lt;destination-entity&gt;</i> | Destination entity name.                                                                                                                                                                                                                                                                                             |
| 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.<br><br>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](#) to check rule configuration validity.

You can change the rule order by using the [move rule \(firewall\)](#).

**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** **move rule (firewall)**  
**commands** **show firewall rule**  
**show firewall rule config-check**

**Command** Version 5.4.7-0.1: **no-state-enforcement** option added.  
**changes**

# 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** The following shows typical output.

## 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)** 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** The following shows typical output.

## 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** The following shows typical output.

## 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** The following shows typical output.

**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** The following shows typical output.

**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** The following shows typical output.

**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** The following shows typical output.

## 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** The following shows typical output.

**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** The following shows typical output.

## 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** The following shows typical output.

## 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** The following shows typical output.

**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** The following shows typical output.

## Example output from the show running-config firewall command

```
awplus#show running-config firewall
firewall
 rule 10 permit ping from public to private
 protect
!
```

# 43

## Application and Entity Commands

- Contents**
- **Introduction** on page 2114
  - **application** on page 2115
  - **dport** on page 2117
  - **dscp** on page 2119
  - **host (network)** on page 2121
  - **icmp-code** on page 2123
  - **icmp-type** on page 2125
  - **ip address (host)** on page 2127
  - **ip subnet** on page 2129
  - **ipv6 address (host)** on page 2131
  - **ipv6 subnet** on page 2134
  - **mac-address (host)** on page 2136
  - **network (zone)** on page 2138
  - **protocol** on page 2140
  - **show application** on page 2142
  - **show application detail** on page 2143
  - **show entity** on page 2145
  - **sport** on page 2148
  - **zone** on page 2150

# Introduction

**Overview** 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.

## Application commands and applicable modes

| Mode                 | Command                                 |
|----------------------|-----------------------------------------|
| Privileged Exec      | <a href="#">show application</a>        |
|                      | <a href="#">show application detail</a> |
| Global Configuration | <a href="#">application</a>             |
| Application Mode     | <a href="#">protocol</a>                |
|                      | <a href="#">icmp-type</a>               |
|                      | <a href="#">icmp-code</a>               |
|                      | <a href="#">sport</a>                   |
|                      | <a href="#">dport</a>                   |

The table below lists the entity commands and their applicable modes.

## Entity commands

| Mode                 | Command                             |
|----------------------|-------------------------------------|
| Privileged Exec      | <a href="#">show entity</a>         |
| Global Configuration | <a href="#">zone</a>                |
| Zone Mode            | <a href="#">network (zone)</a>      |
| Network Mode         | <a href="#">ip subnet</a>           |
|                      | <a href="#">ipv6 subnet</a>         |
|                      | <a href="#">host (network)</a>      |
| Host Mode            | <a href="#">ip address (host)</a>   |
|                      | <a href="#">ipv6 address (host)</a> |

# 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.

You can use the tab key to auto-complete application names.

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><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 destinations 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 <b>max</b> .                                       |

**Mode** Application Mode

**Usage notes** You can have up to 15 **dports** per application. This is counted as follows:

- a single **dport** counts as 1 port
- a range counts as 2 ports
- the keyword **any** counts as 2 ports.

**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.                                  |

## Assured Forwarding (AF) behavior group

|                         | Class 1        | Class 2        | Class 3        | Class 4        |
|-------------------------|----------------|----------------|----------------|----------------|
| Low drop probability    | AF11 (DSCP 10) | AF21 (DSCP 18) | AF31 (DSCP 26) | AF41 (DSCP 34) |
| Medium drop probability | AF12(DSCP 12)  | AF22(DSCP 20)  | AF32(DSCP 28)  | AF42(DSCP 36)  |
| High drop probability   | AF13(DSCP 14)  | AF23(DSCP 22)  | AF33(DSCP 30)  | AF43(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><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)** and **ipv6 address (host)** 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
```

**Related commands**

- ip address (host)**
- ipv6 address (host)**
- mac-address (host)**
- network (zone)**
- show entity**

## 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** 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-number> | Specify an ICMP message code number in the range of 0 to 255. |
| any           | 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.

Domain names will match the most specific FQDN entity available, with subdomains matching less specific FQDNs when necessary.

This functions similarly to a wildcard DNS record. For example, with the FQDN entities 'com,' 'google.com,' and 'maps.google.com' configured, 'microsoft.com' will match 'com,' 'drive.google.com' will match 'google.com,' and 'maps.google.com' will match 'maps.google.com' rather than 'google.com'.

**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, ppp, tunnel, lo, etc.) followed by any character.<br><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 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
```

**Related commands** **network (zone)**  
**show entity**

## 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                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-address&gt;</code>   | The IPv6 address in the format x:x::x:x.                                                                                                                               |
| <code>dynamic</code>                | Dynamic IPv6 address, for example, obtained from a DHCP server.                                                                                                        |
| <code>&lt;domain_name&gt;</code>    | The FQDN to resolve IP addresses for.<br><br>Valid characters are any printable character. If the name contains spaces, then you must enclose it in "quotation marks". |
| <code>&lt;interface_name&gt;</code> | Interface to acquire IP addresses from.                                                                                                                                |

**Mode** Host

**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.

Domain names will match the most specific FQDN entity available, with subdomains matching less specific FQDNs when necessary.

This functions similarly to a wildcard DNS record. For example, with the FQDN entities 'com,' 'google.com,' and 'maps.google.com' configured, 'microsoft.com' will match 'com,' 'drive.google.com' will match 'google.com,' and 'maps.google.com' will match 'maps.google.com' rather than 'google.com'.



**Examples** To add an IPv6 address to the host named '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 the host named '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 the host named '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: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, ppp, tunnel, lo, etc.) followed by any character.<br><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
```

**Related commands** **network (zone)**  
**show entity**

## mac-address (host)

**Overview** Use this command to filter packets that come from particular hosts. You do this by attaching the host's MAC address to the host entity.

This is a useful alternative to filtering by IP address, especially if the host's IP address is allocated dynamically.

You can use this filtering, for example, to increase security by preventing internal sensors from sending information out to the Internet.

You can add multiple MAC addresses for a given host entity, if more than one device is part of the entity.

Use the **no** variant of this command to remove a MAC address from the host.

**Syntax** `mac-address <mac-address>`  
`no mac-address <mac-address>`

| Parameter                        | Description                                                       |
|----------------------------------|-------------------------------------------------------------------|
| <code>&lt;mac-address&gt;</code> | A MAC address to match on, specified in XX:XX:XX:XX:XX:XX format. |

**Default** No MAC addresses are attached to host entities

**Mode** Host

**Usage notes** This feature matches on incoming packets. This means you should use it with Firewall or NAT rules where the entity is in the **from** field.

MAC addresses specified with this command are not used for matching in Web Control or DPI Detailed Counters.

**Example** To add the MAC address 00:00:cd:11:22:33 to the entity named example.cameras.door, use the commands:

```
awplus# configure terminal
awplus(config)# zone example
awplus(config-zone)# network cameras
awplus(config-network)# host door
awplus(config-host)# mac-address 00:00:cd:11:22:33
```

To use this example.cameras.door entity to block traffic from the camera to the Internet, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule deny any from example.cameras.door
to inet
awplus(config-firewall)# protect
```

To remove the MAC address 00:00:cd:11:22:33 from the entity, use the commands:

```
awplus# configure terminal
awplus(config)# zone example
awplus(config-zone)# network cameras
awplus(config-network)# host door
awplus(config-host)# no mac-address 00:00:cd:11:22:33
```

**Related commands** **host (network)**  
**network (zone)**  
**show entity**  
**zone**

**Command changes** Version 5.5.3-1.1: command added

# 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                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <network-name> | Network name.<br><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** and the **ipv6 subnet**.

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](#) 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** The following shows typical output.

## 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
```

## Example output from show application detail for an application

```
awplus#show application detail ping
Name Mark Detail

ping - proto=ICMP type=8 code=0
```

## 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.<br><br>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** The following shows typical output.

## 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** The following shows typical output.

**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** The following shows typical output.

**Example output from the show entity command**

```
awplus#show entity zone1.network1.host1
Host: zone1.network1.host1
Address: 192.168.1.5
```

**Output** When the entity is using dynamic interface addresses, this will be shown in the output:

**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)
```

**Output** When the entity is using dynamic FQDN addresses, this will be shown in the output:

**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 <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 have up to 15 **sports** per application. This is counted as follows:

- a single **sport** counts as 1 port
- a range counts as 2 ports
- the keyword **any** counts as 2 ports.



**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                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <zone-name> | Zone name.<br><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 \(zone\)](#).

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 \(zone\)](#).

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**

# 44

## NAT Commands

- Contents**
- **Introduction** on page 2153
  - **enable (nat)** on page 2154
  - **ip limited-local-proxy-arp** on page 2155
  - **local-proxy-arp** on page 2156
  - **move rule (nat)** on page 2157
  - **nat** on page 2158
  - **rule (nat)** on page 2159
  - **show nat** on page 2164
  - **show nat rule** on page 2165
  - **show nat rule config-check** on page 2167
  - **show running-config nat** on page 2168

# Introduction

**Overview** 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.

## NAT commands and applicable modes

| Mode                 | Command                                    |
|----------------------|--------------------------------------------|
| Privileged Exec      | <a href="#">show nat</a>                   |
|                      | <a href="#">show nat rule</a>              |
|                      | <a href="#">show nat rule config-check</a> |
|                      | <a href="#">show running-config nat</a>    |
| Global Configuration | <a href="#">nat</a>                        |
| NAT Configuration    | <a href="#">enable (nat)</a>               |
|                      | <a href="#">move rule (nat)</a>            |
|                      | <a href="#">rule (nat)</a>                 |

# 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 for Eth, WWAN, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

**Usage** This command allows you to stop MAC address resolution for specified hosts. Limited local proxy ARP works by intercepting ARP requests for the specified hosts and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of the other hosts through ARP requests.

Limited local proxy ARP ensures that the specified devices cannot send traffic that bypasses Layer 3 routing on your device. This gives you control over which hosts may communicate with one another.

**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                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;ip-add/mask&gt;</i> | 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                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| move rule<br><1-65535> | Move the order of a given rule. The rule ID of the given rule must exist.<br><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. |
| to <1-65535>           | 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)**.
- Create NAT rules or change the order of NAT rules, see the **rule (nat)** and the **move rule (nat)**.

**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.<br><br>You can use the tab key to auto-complete application names.                                                                                                                                                                         |
| <source-entity>    | 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.<br><br>You can use the tab key to auto-complete entity names.<br><br>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 |

| Parameter                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | <p>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.</p> <p>In a <b>portfw</b> rule, the source entity may be an entity outside your private network.</p> |
| <i>&lt;destination-entity&gt;</i>        | <p>The destination entity name.</p> <p>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).</p>                                                                                                                                                                                  |
| <i>&lt;source-host-entity&gt;</i>        | <p>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.</p>                                                                                                                                                                                                                         |
| <i>&lt;destination-host-entity&gt;</i>   | <p>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.</p>                                                                                                                                                                                               |
| dport <1-65535>                          | <p>In a <b>portfw</b> rule, modify the destination port to the specified port. (Only for protocols that have ports.)</p>                                                                                                                                                                                                                                                                                                                   |
| <i>&lt;source-subnet-entity&gt;</i>      | <p>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 &lt;translated-subnet-entity&gt; specified.</p>                                                                                                                                                                 |
| <i>&lt;destination-subnet-entity&gt;</i> | <p>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 &lt;translated-subnet-entity&gt; specified.</p>                                                                                                                                                          |
| <i>&lt;translated-subnet-entity&gt;</i>  | <p>In a <b>netmap</b> rule:</p> <p><b>with src:</b> Modify the source-subnet-entity to the specified translated-subnet-</p>                                                                                                                                                                                                                                                                                                                |

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | 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><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)**.

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)** 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** and the **ipv6 subnet** 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** The following shows typical output.

## 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** The following shows typical output.

## 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** The following shows typical output.

**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> . |
| App              | Application name.                                                                                       |
| From             | Source entity.                                                                                          |
| 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** The following shows typical output.

**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** The following shows typical output.

**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** The following shows typical output.

## 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

# 45

## IPS Commands

- Contents**
- **Introduction** on page 2171
  - **alert-thresholding** on page 2172
  - **category action (IPS)** on page 2173
  - **ips** on page 2174
  - **protect (IPS)** on page 2175
  - **provider (IPS)** on page 2176
  - **show ips** on page 2177
  - **show ips categories** on page 2178
  - **show ips categories detail** on page 2181
  - **show running-config ips** on page 2183
  - **sid** on page 2184
  - **update-interval (IPS)** on page 2185

# Introduction

**Overview** 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.

## IPS Commands and Applicable Modes

| Mode                 | Command                                 |
|----------------------|-----------------------------------------|
| Privileged Exec      | <a href="#">show ips</a>                |
|                      | <a href="#">show ips categories</a>     |
|                      | <a href="#">show running-config ips</a> |
| Global Configuration | <a href="#">ips</a>                     |
| IPS Mode             | <a href="#">alert-thresholding</a>      |
|                      | <a href="#">category action (IPS)</a>   |
|                      | <a href="#">protect (IPS)</a>           |

# alert-thresholding

**Overview** Use this command to limit IPS to a maximum of 6 alerts per minute per destination IP address. This prevents IPS alerts from overwhelming the log files.

Use the **no** variant of this command to turn off the limit if you need to log every packet that matches an IPS rule (for example, for debugging purposes).

**Syntax** alert-thresholding  
no alert-thresholding

**Default** Enabled

**Mode** IPS Configuration

**Example** To stop limiting the number of IPS alerts, so that the device logs every packet that matches an IPS rule, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no alert-thresholding
```

To limit the number of IPS alerts again, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# alert-thresholding
```

**Related commands** [show log](#)  
[show ips](#)

**Command changes** Version 5.5.0-2.1: command added



# 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> 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 Configuration

**Examples** To drop packets 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 the 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)**.
- Configure an action for specified categories, see the **category action (IPS)**.

**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](#) 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** [show ips](#)  
**Commands** [show running-config ips](#)

# provider (IPS)

**Overview** Use this command to configure an IPS (Intrusion Prevention System) provider.

A provider is a third-party vendor that supplies a comprehensive rule set for detecting and blocking advanced threats.

Rule sets include extensive signatures. This is where a previously known event can be characterised in some way that can be used to detect if the event happens again. The signature database is kept up-to-date to ensure the effectiveness of the detection.

Use the **no** variant of this command to disable a provider.

**Syntax** provider proofpoint  
no provider

| Parameter  | Description                       |
|------------|-----------------------------------|
| proofpoint | Use Proofpoint signatures in IPS. |

**Mode** IPS Configuration

**Example** To configure Proofpoint as the provider, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# provider proofpoint
```

To unset a provider, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no provider
```

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

**Command changes** Version 5.5.2-2.1: command added

# 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** The following shows typical output.

## Example output from show ips

```
awplus#show ips
Status: Enabled (Active)
Events: 4
Alert Thresholding: Enabled
```

## Parameters in the output from show ips

| Parameter          | Description                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alert Thresholding | Either Enabled or Disabled. When enabled, IPS produces a maximum of 6 alerts per minute per destination IP address. This prevents IPS alerts from overwhelming the log files. To enable or disable this, use the <a href="#">alert-thresholding</a> command. |

**Related commands** [show ips categories detail](#)

# 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 command 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** The following shows typical output.

**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                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| checksu             | 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 length, HTTP invalid response chunk length, HTTP status 100-Continue already seen, HTTP unable to match response to request, HTTP invalid server port in request.                                              |
| 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 and 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 |

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | 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 length 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 ips categories detail

**Overview** Use this command to show the detailed information about IPS (Intrusion Prevention System) categories.

**Syntax** show ips categories detail [<category-name>]

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <category-name> | Optional - enter a category name to only show information about a specific category. <ul style="list-style-type: none"><li>Category names are case sensitive and can be up to 64 characters long composed of printable ASCII characters.</li><li>A category is a label that helps to classify the nature of traffic, for example, whether it is spammer, bot, or spyware and so on.</li></ul> |

**Mode** Privileged Exec

**Example** To show detailed information about all the IPS categories, use the command:

```
awplus# show ips categories detail
```

**Output** The following shows typical output.

## Example output from show ips categories detail

| awplus#show ips categories detail |        |       |                                                                                                                                                                                                                                                                      |
|-----------------------------------|--------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category (* = invalid)            | Action | Rules | Description                                                                                                                                                                                                                                                          |
| 3coresec                          | alert  | 33    | IP block list signatures automatically generated from the 3CORESec team's Honeypots                                                                                                                                                                                  |
| activex                           | alert  | 242   | Signatures for protection against attacks on Microsoft ActiveX controls and exploits targeting vulnerabilities in ActiveX controls                                                                                                                                   |
| attack_response                   | alert  | 692   | Signatures to identify responses indicative of intrusion. Examples include but not limited to LMHost file download, presence of web banners and the detection of Metasploit Meterpreter kill command. These are designed to catch the results of a successful attack |
| botcc                             | alert  | 24    | (Bot Command and Control) Signatures that are autogenerated from several sources of known and confirmed active botnet and other Command and Control (C2) hosts. This category is updated daily. Primarily sourced from Shadowserver.org                              |
| ...                               |        |       |                                                                                                                                                                                                                                                                      |

**Example** To show detailed information about the IPS category 'activex', use the command:

```
awplus# show ips categories detail activex
```

**Output** The following shows typical output.

**Example output from show ips categories detail activex**

```
awplus#show ips categories detail activex
Category (* = invalid) Action Rules Description

activex alert 242 Signatures for protection against
 attacks on Microsoft ActiveX controls
 and exploits targeting vulnerabilities
 in ActiveX controls
```

**Related commands** [category action \(IPS\)](#)  
[show ips categories](#)

**Command changes** Version 5.5.2-2.1: command added

# show running-config ips

**Overview** Use this command to show the configuration commands that have been used to configure IPS.

**Syntax** show running-config ips

**Mode** Privileged Exec

**Examples** To show the commands that have been used to configure IPS, use the command:

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

**Output** The following shows typical output.

**Example output from the show running-config ips command**

```
awplus#show running-config ips
ips
 protect
!
```

# sid

**Overview** Use this command to configure a rule's action via its Signature ID (SID). Rule actions default to their category action. For example, if the IPS category 'smtp-events' is set to 'deny', then you can configure the SID '2220006' to be disabled so that the signature is not blocked.

The IPS log contains the SID for each configured IPS category.

Use the **no** variant of this command to return a SID to using the category's configured action.

**Syntax** `sid <1-2147483647> action {alert|deny|disable}`  
`no sid <1-2147483647>`

| Parameter      | Description                                                                  |
|----------------|------------------------------------------------------------------------------|
| <1-2147483647> | The SID of the rule to override.                                             |
| alert          | Generate a log message, this is the default action.                          |
| deny           | Drop the matching packets. No error message is sent back to the source host. |
| disable        | No action will be taken for matching packets.                                |

**Default** Alert.

**Mode** IPS Configuration

**Example** To disable the IPS rule for SID 2220006, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# sid 2220006 action disable
```

To return the IPS rule for SID 2220006 back to the action of its category, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no sid 2220006 action
```

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

**Command changes** Version 5.5.2-2.1: command added

# update-interval (IPS)

**Overview** Use this command to configure an update check interval for the IPS provider resource files.

A provider is a third-party vendor that supplies a comprehensive rule set for detecting and blocking advanced threats.

Use the **no** variant of this command to use the default update interval of IPS provider resources.

**Syntax** `update-interval {minutes <10-525600>|hours <1-8760>|  
days <1-365>|weeks <1-52>|never}  
no update-interval`

| Parameter           | Description                                    |
|---------------------|------------------------------------------------|
| minutes <10-525600> | Update interval from 10 through 52600 minutes  |
| hours <1-8760>      | Update interval from 1 hour through 8760 hours |
| days <1-365>        | Update interval from 1 day through 365 days    |
| weeks <1-52>        | Update interval from 1 week through 52 weeks   |
| never               | Never update the resource.                     |

**Default** 1 hour.

**Mode** IPS Configuration

**Usage notes** The Update Manager will perform an update check for a resource when triggered by an update check interval. It 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.

The Update Manager will revert to last known good resource file if installation of an updated resource fails.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

**Example** To check and update the IPS provider resource files once a week, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# update-interval weeks 1
```

To disable updating the IPS provider resource files, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# update-interval never
```

To restore the default update interval for IPS provider resource files, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no update-interval
```

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

**Command changes** Version 5.5.2-2.1: command added

# 46

## URL Filtering Commands

- Contents**
- **Introduction** on page 2188
  - **blacklist** on page 2189
  - **log url-requests** on page 2190
  - **protect (url-filter)** on page 2191
  - **show running-config url-filter** on page 2192
  - **show url-filter** on page 2193
  - **url-filter reload custom-lists** on page 2194
  - **url-filter** on page 2195
  - **whitelist (url-filter)** on page 2196

# Introduction

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

If you subscribe to a blacklist service, you can create custom blacklists to block additional URLs not in the third-party provider's blacklist or custom whitelists to allow URLs that the service blocks.

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.

## URL filtering commands and applicable modes

| Mode                     | Command                                        |
|--------------------------|------------------------------------------------|
| Privileged Exec          | <a href="#">show running-config url-filter</a> |
|                          | <a href="#">show url-filter</a>                |
|                          | <a href="#">url-filter reload custom-lists</a> |
| Global Configuration     | <a href="#">url-filter</a>                     |
| URL Filter Configuration | <a href="#">blacklist</a>                      |
|                          | <a href="#">protect (url-filter)</a>           |
|                          | <a href="#">whitelist (url-filter)</a>         |



# 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. |

**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**  
**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** The following shows typical output.

## 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. |

**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

**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.



# 47

## Application Awareness Commands

- Contents**
- **Introduction** on page 2198
  - **counters detailed** on page 2199
  - **dpi** on page 2200
  - **enable (dpi)** on page 2201
  - **hostname (application)** on page 2203
  - **provider (dpi)** on page 2204
  - **show dpi** on page 2205
  - **show dpi statistics** on page 2206
  - **show running-config dpi** on page 2208
  - **web-categorization** on page 2209

# Introduction

This chapter provides an alphabetical reference of commands used to configure application awareness, which uses Deep Packet Inspection (DPI). For more information about application awareness and a configuration example, see the [Application Awareness Feature Overview and Configuration\\_Guide](#).

## counters detailed

**Overview** Use this command to enable the display of transmit and receive counters for each entity in DPI mode.

Once you have enabled detailed counters, you can use the command **show dpi statistics <entity-name>** to display statistics for different applications on individual entities (zones, networks or hosts). This is called DPI statistics per entity.

Use the **no** variant of this command to disable DPI statistics per entity.

**Syntax** counters detailed  
no counters detailed

**Default** Disabled

**Mode** DPI Configuration

**Usage notes** These counters will require system resources and should only be configured when required. Use the **no** variant to turn them off when not required.

**Example** To configure DPI statistics per entity, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
awplus(config-dpi)# counters detailed
```

To disable DPI statistics per entity, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no counters detailed
```

**Related commands** **show dpi statistics**

**Command changes** Version 5.4.9-1.1: command added

# dpi

**Overview** Use this command to enter DPI Configuration mode to configure DPI for application awareness.

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

**Syntax** dpi  
no dpi

**Mode** Global Configuration

**Usage notes** In DPI Configuration mode, you can:

- Set the DPI provider, using the **provider (dpi)** command.
- Enable DPI, using the **enable (dpi)** command.

**Examples** To begin configuring DPI, use the commands:

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

To remove all DPI configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no dpi
```

**Command changes** Version 5.4.7-2.1: command added

# enable (dpi)

**Overview** Use this command to enable DPI for application awareness.

Use the **no** variant of this command to disable DPI without losing existing DPI configuration.

**Syntax** enable  
no enable

**Default** DPI is disabled by default.

**Mode** DPI Configuration

**Usage notes** Use the **provider (dpi)** command to configure the DPI provider before enabling DPI.

When DPI is enabled, it can classify network traffic and identify today's most common applications.

DPI itself does not control or apply rules to the traffic. You can use the application awareness provided by DPI for:

- Network visibility
- Application Control, using the **rule (firewall)** command to enforce security policy and apply rules to the DPI applications
- Traffic Control, using the traffic control rules
- Policy-based Routing (PBR), using the PBR rules.

You can use the **show dpi statistics** command to show statistics for the applications being inspected by DPI.

For more information about configuring and using DPI, see the [Application Awareness Feature Overview and Configuration Guide](#).

**Examples** To enable DPI to use the built-in library, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
```

To disable DPI, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no enable
```

**Related commands**    **provider (dpi)**  
                          **show dpi**  
                          **show running-config dpi**

**Command changes**    Version 5.4.7-2.1: command added

# hostname (application)

**Overview** Use this command to specify a hostname used by an application.

An application is a high-level definition of different types of applications being transported by network traffic. For example, social networking.

You associate a hostname or multiple hostnames with an application.

Use the **no** variant of this command to remove a hostname from an application.

**Syntax** hostname <hostname>  
no hostname

| Parameter  | Description                                                    |
|------------|----------------------------------------------------------------|
| <hostname> | The hostname expressed as a URI (Uniform Resource Identifier). |

**Default** Not set.

**Mode** Application Configuration

**Example** To specify a hostname for the Stuff application, use the commands:

```
awplus# configure terminal
awplus(config)# application Stuff
awplus(config-application)# hostname stuff.co.nz
```

To specify an application for Youtube with multiple hostnames, use the commands:

```
awplus# configure terminal
awplus(config)# application Youtube
awplus(config-application)# hostname youtube.com
awplus(config-application)# hostnameyoutu.be
```

To remove a hostname from an application for Youtube, use the commands:

```
awplus# configure terminal
awplus(config)# application Youtube
awplus(config-application)# no hostname youtube.com
```

**Related commands** [application](#)

**Command changes** Version 5.5.2-0.1: command added

## provider (dpi)

**Overview** Use this command to set the DPI provider for the library of applications used for DPI to the built-in library predefined in device's operating system. Application awareness uses DPI, if enabled, to identify applications by matching packets to a library of application signatures.

**Syntax** provider built-in

**Default** No provider is set by default.

**Mode** DPI Configuration

**Usage notes** You can use the **show application** command and the **show application detail** command to view all applications that the device recognizes. If DPI is enabled, the show commands can include the commands in the library specified with this provider command.

Note that custom applications override DPI applications, which override AlliedWare Plus predefined applications. For more information about applications, see the **application** command.

Note that you need to use this command before using the **enable (dpi)** command to enable DPI.

**Examples** To set the DPI provider to the built-in library of application signatures, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
```

**Related commands**

- enable (dpi)**
- show application detail**
- show dpi**
- show running-config dpi**

**Command changes** Version 5.4.7-2.1: command added



# show dpi

**Overview** Use this command to show the DPI configuration state.

**Syntax** show dpi

**Mode** Privileged Exec

**Examples** To show information about the DPI configuration and provider's library, use the command:

```
awplus# show dpi
```

**Output** The following shows typical output.

**Example output from show dpi with DPI enabled and the provider set to built-in**

```
awplus#show dpi
Status: running
Provider: built-in
```

**Parameters in the output from show dpi**

| Parameter | Description                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status    | The status of DPI: <ul style="list-style-type: none"><li>• running—DPI is running – DPI is enabled, and the provided library is available</li><li>• disabled—DPI is disabled</li></ul> |
| Provider  | The provider for the library of application signatures used to identify applications.                                                                                                  |

**Related commands** [enable \(dpi\)](#)  
[provider \(dpi\)](#)

**Command changes** Version 5.4.7-2.1: command added

## show dpi statistics

**Overview** Use this command to display statistics for each application being inspected by DPI. This command gives you counts of the total number of packets and bytes of the applications being inspected by DPI. You can use the **rule (firewall)** command, traffic control rules or PBR rules to apply rules to the DPI applications.

You can also use this command to display application DPI statistics for an individual entity (zone, network or host). Enable this with the **counters detailed** command.

**Syntax** show dpi statistics [<entity-name>]

| Parameter     | Description                                                                        |
|---------------|------------------------------------------------------------------------------------|
| <entity-name> | The name of an individual entity, for example the name of a zone, network or host. |

**Mode** Privileged Exec

**Examples** To display the statistics for each application being inspected by DPI, use the command:

```
awplus# show dpi statistics
```

**Output** The following shows typical output.

**Example output from the show dpi statistics command on the console.**

|                            |         |       |
|----------------------------|---------|-------|
| awplus#show dpi statistics |         |       |
| Application                | Packets | Bytes |
| -----                      |         |       |
| http                       | 30      | 2020  |
| icmp                       | 348     | 29232 |
| telnet                     | 45      | 2553  |

To show information about the DPI statistics for an individual entity, for example the entity "joeb", use the command:

```
awplus# show dpi statistics joeb
```

**Examples output from show dpi statistics**

|                                 |            |            |          |          |
|---------------------------------|------------|------------|----------|----------|
| awplus#show dpi statistics joeb |            |            |          |          |
| Statistics for entity: joeb     |            |            |          |          |
| Application                     | TX Packets | RX Packets | TX Bytes | RX Bytes |
| -----                           |            |            |          |          |
| youtube                         | 15413      | 16542      | 15412    | 45123645 |
| google                          | 15413      | 654        | 12205    | 451254   |
| facebook                        | 4115       | 8153       | 1100     | 123588   |
| twitter                         | 15413      | 4865       | 35459    | 24236    |

**Parameters in the output from show dpi statistics**

| Parameter   | Description                                |
|-------------|--------------------------------------------|
| Application | The application associated with the packet |
| TX Packets  | Transmitted packets                        |
| RX Packets  | Received packets                           |
| TX Bytes    | Bytes transmitted                          |
| RX Bytes    | Bytes received                             |

**Related commands** [counters detailed](#)

**Command changes** Version 5.4.7-2.1: command added  
Version 5.4.9-1.1: entity parameter added

# show running-config dpi

**Overview** Use this command to show the configuration commands that have been used to configure DPI.

**Syntax** show running-config dpi

**Mode** Privileged Exec

**Examples** To show the configuration commands that have been used to configure DPI, use the command:

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

**Output** The following shows typical output.

## Example output from the show running-config dpi command

```
awplus#show running-config dpi
dpi
 provider built-in
 enable
!
```

**Command changes** Version 5.4.7-2.1: command added

# web-categorization

**Overview** Use this command to configure DPI's web-categorization and optionally a provider. DPI's web-categorization classifies network traffic into provider defined categories (e.g. online auctions, social networking) and/or user defined custom categories.

Use Web-categorization to help protect users on the network based on the type of website they access.

Use the **no** variant of this command to disable web-categorization.

**Syntax** web-categorization [digital-arts|opentext]  
no web-categorization

| Parameter    | Description                                                     |
|--------------|-----------------------------------------------------------------|
| digital-arts | Use the Digital Arts provider and their database of categories. |
| opentext     | Use the OpenText provider and their database of categories.     |

**Default** Disabled

**Mode** DPI Configuration

**Usage notes** Web-categorization requires a Web Control subscription license.

**Examples** To enable DPI Web-categorization and set the provider to Digital Arts, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization digital-arts
```

To enable DPI Web-categorization and set the provider to OpenText, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization opentext
```

To enable DPI Web-categorization with no external provider, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization
```

To disable DPI Web-categorization, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no web-categorization
```

**Related commands** **enable (dpi)**  
**show dpi statistics**  
**show running-config dpi**  
**show dpi**

**Command changes** Version 5.5.3-0.1: **opentext** parameter added  
Version 5.5.2-0.1: command added

# **Part 8: Virtual Private Networks (VPNs)**

# 48

## IPsec Commands

- Contents**
- **Introduction** on page 2214
  - **clear isakmp sa** on page 2215
  - **crypto ipsec profile** on page 2216
  - **crypto isakmp key** on page 2218
  - **crypto isakmp peer** on page 2222
  - **crypto isakmp profile** on page 2225
  - **debug isakmp** on page 2227
  - **dpd-interval** on page 2229
  - **dpd-timeout** on page 2230
  - **interface tunnel (IPsec)** on page 2231
  - **lifetime (IPsec Profile)** on page 2232
  - **lifetime (ISAKMP Profile)** on page 2233
  - **no debug isakmp** on page 2234
  - **pfs** on page 2235
  - **rekey** on page 2237
  - **show debugging isakmp** on page 2239
  - **show interface tunnel (IPsec)** on page 2240
  - **show ipsec counters** on page 2241
  - **show ipsec peer** on page 2242
  - **show ipsec policy** on page 2244
  - **show ipsec profile** on page 2245
  - **show ipsec sa** on page 2247
  - **show isakmp counters** on page 2248
  - **show isakmp key (IPsec)** on page 2249
  - **show isakmp peer** on page 2250
  - **show isakmp profile** on page 2251
  - **show isakmp sa** on page 2253
  - **show tunnel inline-processing counters** on page 2254
  - **transform (IPsec Profile)** on page 2257
  - **transform (ISAKMP Profile)** on page 2259
  - **tunnel destination (IPsec)** on page 2261
  - **tunnel inline-processing** on page 2263
  - **tunnel local name (IPsec)** on page 2264
  - **tunnel local selector** on page 2265
  - **tunnel mode ipsec** on page 2267
  - **tunnel oper-status-control** on page 2268
  - **tunnel protection ipsec (IPsec)** on page 2271



- **tunnel remote name (IPsec)** on page 2272
- **tunnel remote selector** on page 2273
- **tunnel security-reprocessing** on page 2276
- **tunnel selector paired** on page 2277
- **tunnel source (IPsec)** on page 2278
- **undebg isakmp** on page 2280
- **version (ISAKMP)** on page 2281

# Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Internet Protocol Security (IPsec) tunnel.

For introductory information about IPsec tunnel in AlliedWare Plus, including overview and configuration information, see the:

- [\*\*Internet Protocol Security \(IPsec\) Feature Overview and\\_Configuration Guide\*\*](#)

## clear isakmp sa

**Overview** Use this command to delete Internet Security Association Key Management Protocol (ISAKMP) Security Associations (SAs). SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPsec peers. For more information about SA, see the Internet Protocol Security (IPsec) Feature Overview and Configuration Guide.

**Syntax** `clear [crypto] isakmp sa [peer <ipv4-addr>|<ipv6-addr>|<hostname>] [force]`

| Parameter   | Description                                                          |
|-------------|----------------------------------------------------------------------|
| <ipv4-addr> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <ipv6-addr> | Destination IPv6 address. The IPv4 address uses the format X:X::X:X. |
| <hostname>  | Destination host name.                                               |
| force       | Force to clear ISAKMP SAs without negotiating with the peer.         |

**Mode** Privileged Exec

**Examples** To delete the ISAKMP security associations at the peer for an IPv6 address, use the command:

```
awplus# clear isakmp sa peer 2001:0db8::1
```

To delete the ISAKMP security associations at the peer for an IPv4 address, use the command:

```
awplus# clear isakmp sa peer 192.168.2.1
```

To delete the ISAKMP security associations at the peer for a host name, use the command:

```
awplus# clear isakmp sa peer remote.example.com
```

**Related commands** [crypto isakmp key](#)  
[show isakmp sa](#)

**Command Changes** Version 5.4.7-0.1: Parameter <hostname> added for DDNS feature.

# crypto ipsec profile

**Overview** Use this command to configure a custom IPsec profile.

An IPsec profile comprises one or more transforms that can be configured by using the **transform (IPsec Profile)** command.

Use the **no** variant to delete a previously created profile.

**Syntax** `crypto ipsec profile <profile_name>`  
`no crypto ipsec profile <profile_name>`

| Parameter      | Description                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <profile_name> | Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore). |

**Default** The default IPsec profile with transforms in order of preference is listed in the following table. Which IPsec profile will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. Note that you cannot delete or edit the default profile. Expiry time of 8 hours applies to the default IPsec profile.

## IPsec default profile

| Attribute            | Transform 1 | Transform 2 | Transform 3 | Transform 4 | Transform 5 | Transform 6 |
|----------------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Protocol             | ESP         | ESP         | ESP         | ESP         | ESP         | ESP         |
| Encryption (all CBC) | AES256      | AES256      | AES128      | AES128      | 3DES        | 3DES        |
| Integrity (all HMAC) | SHA256      | SHA1        | SHA256      | SHA1        | SHA256      | SHA1        |

**Mode** Global Configuration

**Examples** To configure a custom IPsec profile for establishing IPsec SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# transform 2 protocol esp integrity
sha1 encryption 3des
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto ipsec profile my_profile
```

**Related commands**

- lifetime (IPsec Profile)**
- show ipsec profile**
- transform (IPsec Profile)**

## crypto isakmp key

**Overview** Use this command to configure an ISAKMP authentication key. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

You must configure this key whenever you specify authentication keys in an (Internet Key Exchange) IKE policy and at both peers.

This command specifies both the value of the key and also an identifier (the hostname, address or policy parameters). This identifier is used to decide which key to use for a particular ISAKMP message exchange.

See the Usage section below for more information, and see the following guides for examples:

- [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#)
- [GRE and Multipoint VPNs Feature Overview and Configuration Guide](#)

Use the **no** variant to remove a key.

**Syntax** `crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]`  
`no crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]`  
`crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]`  
`no crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]`  
`crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]`  
`no crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]`

| Parameter                        | Description                                                                                                                                                                                                                    |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>crypto</code>              | Security specific command.                                                                                                                                                                                                     |
| <code>isakmp</code>              | Internet Security Association Key Management Protocol provides a common framework for key management implementations.                                                                                                          |
| <code>key</code>                 | Pre-shared key (PSK) or Extensible Authentication Protocol (EAP).                                                                                                                                                              |
| <code>&lt;key&gt;</code>         | Specify the key. Use any combination of alphanumeric characters up to 128 bytes.                                                                                                                                               |
| <code>8</code>                   | Specifies that an encrypted key follows.                                                                                                                                                                                       |
| <code>&lt;hostname&gt;</code>    | A hostname (e.g. example.com).                                                                                                                                                                                                 |
| <code>&lt;ipv4-addr&gt;</code>   | IPv4 address. The IPv4 address uses the format A.B.C.D.                                                                                                                                                                        |
| <code>&lt;ipv6-addr&gt;</code>   | IPv6 address. The IPv6 address uses the format X:X::X:X.                                                                                                                                                                       |
| <code>&lt;policy-name&gt;</code> | The local policy name. This is the name of the tunnel (e.g. tunnel2).                                                                                                                                                          |
| <code>type</code>                | ISAKMP key type                                                                                                                                                                                                                |
| <code>eap</code>                 | 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. |
| <code>psk</code>                 | Pre-shared Key (default)                                                                                                                                                                                                       |

**Default** ISAKMP keys do not exist.

**Mode** Global Configuration

**Usage notes** Use this command to configure an authentication key for use with the ISAKMP protocol.

Before a tunnel can be protected by IPsec, each endpoint of the tunnel must verify that they are communicating with an authorized entity. ISAKMP uses authentication keys in the initial handshake between peers to ensure both endpoints are allowed to communicate.

This command specifies both the value of the key and also an identifier which is used to decide which key to use for a particular ISAKMP message exchange. Because the responding endpoint does not identify itself to the local device until after the key is used, it is important that the key identifier is part of the tunnel configuration on the initiating device.

The tunnel configuration parameter used to select which key to use when negotiating IPsec protection for that tunnel is in priority order:

- 1. tunnel remote name**
- 2. tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)
- 3. tunnel local name**
- 4. tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

For point-to-point tunnels, we recommend you configure local and remote names on the tunnels. Then use the remote name of the other device to identify the authentication keys on the local device.

For point-to-multipoint tunnels, it may be necessary to identify the authentication key by the local name of the tunnel, if the ISAKMP negotiation is to be initiated by that tunnel. This is because it is not possible to configure multiple remote names. However, it is possible to use the expected remote addresses or names of the remote initiating tunnels to identify keys. This is because the remote tunnel will identify itself when it initiates a connection.



**Examples** To configure a pre-shared authentication key of “friend”, using a hostname, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname
mypeer@my.domain.com
```

To remove that pre-shared key, use the commands below:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend hostname
mypeer@my.domain.com
```

To configure a pre-shared already-encrypted authentication key, using an IPv4 address, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key 8 Nhe6ioQmzbysQaJr6Du+cA==
address 192.168.1.2
```

To configure a pre-shared key, using the local policy “tunnel2”, use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend policy tunnel2
```

To remove that key, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend policy tunnel2
```

To configure an ISAKMP key using EAP, enter the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname example.com
type eap
```

**Related commands** [show isakmp key \(IPsec\)](#)  
[tunnel destination \(IPsec\)](#)  
[tunnel local name \(IPsec\)](#)  
[tunnel remote name \(IPsec\)](#)

**Command changes** Version 5.4.9-0.1: **type** parameter added  
Version 5.4.9-1.1: **policy** parameter added

## crypto isakmp peer

**Overview** Use this command to configure a peer to use a specific ISAKMP profile.  
Use the **no** variant to set the peer back to using the default profile.

**Syntax** `crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile <profile-name>`  
`no crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile`  
`crypto isakmp peer dynamic profile <profile-name>`  
`no crypto isakmp peer dynamic profile`  
`crypto isakmp peer hostname <hostname> profile <profile-name>`  
`no crypto isakmp peer hostname <hostname> profile`  
`crypto isakmp peer policy <policy-name> profile <profile-name>`  
`no crypto isakmp peer policy <policy-name> profile`

| Parameter                         | Description                                                                |
|-----------------------------------|----------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code>    | IPv4 address. The IPv4 address uses the format A.B.C.D.                    |
| <code>&lt;ipv6-addr&gt;</code>    | IPv6 address. The IPv6 address uses the format X:X::X:X.                   |
| <code>dynamic</code>              | Remote endpoint with a dynamic IP address.                                 |
| <code>&lt;hostname&gt;</code>     | Remote endpoint with a host name as the destination.                       |
| <code>&lt;policy-name&gt;</code>  | The name of a local policy. This is the name of the tunnel (e.g. tunnel2). |
| <code>&lt;profile-name&gt;</code> | Profile name.                                                              |

**Default** By default, all peers use the default profile.

**Mode** Global Configuration

**Usage notes** Use this command to configure a peer to use a specific ISAKMP profile.

When IPsec protection is applied to a tunnel, an ISAKMP profile is selected for use when IPsec parameters need to be negotiated. This profile is chosen when the tunnel first becomes active, and so must be selected based on local configuration only.

The tunnel configuration parameter used to select which ISAKMP profile to use when negotiating IPsec protection for that tunnel is in the following priority order:

1. **tunnel destination dynamic** (if a dynamic profile has been configured)
2. **tunnel endpoint dynamic** (if a dynamic profile has been configured)
3. **tunnel remote name**
4. **tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)
5. **tunnel endpoint <ipv4-address>**
6. **tunnel local name**
7. **tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)
8. **tunnel destination <hostname>** (if the hostname is not specified)
9. **tunnel endpoint <hostname>** (if the hostname is not specified)

**Examples** To configure a profile for a peer, using a dynamic IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer dynamic profile peer_profile
```

To set the profile for the peer back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer dynamic profile
```

To configure a profile for a peer, using a local policy name of "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer policy tunnel2 profile peer-profile
```

To set the profile for the peer back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer policy tunnel2 profile
```

**Related commands** **show isakmp peer**  
**tunnel destination (IPsec)**  
**tunnel local name (IPsec)**  
**tunnel source (IPsec)**  
**tunnel remote name (IPsec)**

**Command Changes** Version 5.4.7-0.1: **hostname** parameter added.  
Version 5.4.9-1.1: **policy** parameter added.

# crypto isakmp profile

**Overview** Use this command to configure a custom ISAKMP profile.

An ISAKMP profile comprises one or more transforms that can be configured by using the **transform (ISAKMP Profile)** command.

Use the **no** variant to delete a previously created profile.

**Syntax** `crypto isakmp profile <profile_name>`  
`no crypto isakmp profile <profile_name>`

| Parameter      | Description                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <profile_name> | Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore). |

**Default** Which ISAKMP profile transform will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. For more information about default ISAKMP profiles, see the following table. Note that you cannot delete or edit the default profile. Expiry time of 24 hours applies to the default profile.

## 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** To enable ISAKMP debugging, use the following command:

```
awplus# debug crypto isakmp all
```

**Output** The following shows typical output.

**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                                                               |
|-----------|---------------------------------------------------------------------------|
| <0-65535> | Specify a tunnel interface index identifier in the range from 0 to 65535. |

**Default** Tunnel interfaces do not exist.

**Mode** Global Configuration

**Usage notes** After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Note that you need to designate a tunnel mode, tunnel source address, tunnel destination address, IP address of tunnel interface and use **tunnel protection ipsec (IPsec)** command to encrypt and authenticate the packets travelling though the tunnel.

**Examples** To configure an IPsec tunnel interface with index 100, enter the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel100
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the IPsec tunnel interface tunnel100, enter the commands below:

```
awplus# configure terminal
awplus(config)# no interface tunnel100
```

**Command changes** Version 5.4.7-2.1: increased range for **tunnel** index identifier.

# lifetime (IPsec Profile)

**Overview** Use this command to specify a lifetime for an IPsec SA.

Lifetime measures how long the IPsec SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (28800 seconds).

**Syntax** `lifetime seconds <300-31449600>`  
`no lifetime seconds`

| Parameter                         | Description          |
|-----------------------------------|----------------------|
| <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** The following shows typical output.

## 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** The following shows typical output.

## Example output from the show interface tunnel command

```
awplus#show interface tunnel2
Interface tunnel2
 Link is UP, administrative state is UP
 Hardware is Tunnel
 IPv4 address 192.168.1.2/30
 index 23 metric 1 mtu 1438
 <UP,RUNNING,MULTICAST>
 VRF Binding: Not bound
 SNMP link-status traps: Disabled
 Bandwidth 1g
 Tunnel source eth1 (200.1.45.1), destination 200.1.15.1
 Tunnel name local 200.1.45.1, remote 200.1.15.1
 Tunnel traffic selectors (ID, local, remote)
 1 0.0.0.0/0 0.0.0.0/0
 Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
 Checksumming of packets disabled, DF bit set, path MTU discovery disabled
 Tunnel protection via IPsec (profile "default")
 Tunnel inline-processing enabled
 Router Advertisement is disabled
 Router Advertisement default routes are accepted
 Router Advertisement prefix info is accepted
 input packets 0, bytes 0, dropped 0, multicast packets 0
 output packets 0, bytes 0, multicast packets 0, broadcast packets 0
 input average rate : 30 seconds 0 bps, 5 minutes 0 bps
 output average rate: 30 seconds 0 bps, 5 minutes 0 bps
 Time since last state change: 0 days 00:00:07
```

**Related commands** interface tunnel (IPsec)

# show ipsec counters

**Overview** Use this command to show IPsec counters.

**Syntax** show [crypto] ipsec counters

| Parameter | Description                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------|
| crypto    | Security specific command.                                                                           |
| ipsec     | Internet Protocol Security defines the protection of IP packets using encryption and authentication. |
| counters  | Show IPsec transformation statistic.                                                                 |

**Mode** Privileged Exec

**Examples** To show IPsec counters, enter the command below:

```
awplus# show ipsec counters
```

**Output** The following shows typical output.

## Example output from the show ipsec counters command

```
awplus#show ipsec counters
Name Value

InError 0
InBufferError 0
InHdrError 0
InNoStates 0
InStateProtoError 0
InStateModeError 0
InStateSeqError 0
InStateExpired 0
InStateMismatch 0
InStateInvalid 0
InTmplMismatch 0
InNoPols 0
InPolBlock 0
InPolError 0
OutError 0
OutBundleGenError 0
OutBundleCheckError 0
OutNoStates 0
OutStateProtoError 0
OutStateModeError 0
OutStateSeqError 0
OutStateExpired 0
OutPolBlock 0
OutPolDead 0
OutPolError 0
FwdHdrError 0
```

# show ipsec peer

**Overview** Use this command to show IPsec information on a per peer basis.

**Syntax** show [crypto] ipsec peer [<hostname>|<ipv4-addr>|<ipv6-addr>]

| Parameter   | Description                                                          |
|-------------|----------------------------------------------------------------------|
| crypto      | Security specific command.                                           |
| peer        | Remote endpoint.                                                     |
| <hostname>  | Destination hostname.                                                |
| <ipv4-addr> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <ipv6-addr> | Destination IPv6 address. The IPv6 address uses the format X:X::X:X. |

**Mode** Privileged Exec

**Examples** To show IPsec information on a per peer basis, enter the command below:

```
awplus# show ipsec peer 172.16.0.1
```

**Output** The following shows typical output.

**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** The following shows typical output.

## 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** The following shows typical output.

**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** The following shows typical output.

**Example output from the show ipsec profile my\_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** The following shows typical output.

### 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** The following shows typical output.

## Example output from the show isakmp counters command

```
awplus#show isakmp counters
Name Value

ikeInitRekey 0
ikeRspRekey 0
ikeChildSaRekey 0
ikeInInvalid 0
ikeInInvalidSpi 0
ikeInInitReq 0
ikeInInitRsp 0
ikeOutInitReq 0
ikeOutInitRsp 0
ikeInAuthReq 0
ikeInAuthRsp 0
ikeOutAuthReq 0
ikeOutAuthRsp 0
ikeInCrChildReq 0
ikeInCrChildRsp 0
ikeOutCrChildReq 0
ikeOutCrChildRsp 0
ikeInInfoReq 0
ikeInInfoRsp 0
ikeOutInfoReq 0
ikeOutInfoRsp 0
```

# show isakmp key (IPsec)

**Overview** Use this command to show ISAKMP authentication keys. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

**Syntax** show [crypto] isakmp key

| Parameter | Description                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------|
| crypto    | Security specific command.                                                                                            |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| key       | Pre-shared key (PSK), or Extensible Authentication Protocol (EAP).                                                    |

**Mode** Privileged Exec

**Examples** To show the ISAKMP keys, enter the command below:

```
awplus# show isakmp key
```

**Output** The following shows typical output.

## Example output from the show isakmp key command

| awplus#show isakmp key |           |            |
|------------------------|-----------|------------|
| Hostname/IP address    | PSK       | EAP        |
| -----                  |           |            |
| 10.1.1.1               | mykeyone  | mykeytwo   |
| 10.1.5.1               | mykeyfive | -          |
| 10.1.7.1               | -         | mykeyseven |

**Related commands** [crypto isakmp key](#)

# show isakmp peer

**Overview** Use this command to show ISAKMP profile and key status for ISAKMP peers.

**Syntax** show isakmp peer [*<hostname>* | *<ipv4-addr>* | *<ipv6-addr>*]

| Parameter                | Description                                                          |
|--------------------------|----------------------------------------------------------------------|
| <i>&lt;hostname&gt;</i>  | Destination hostname.                                                |
| <i>&lt;ipv4-addr&gt;</i> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <i>&lt;ipv6-addr&gt;</i> | 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** The following shows typical output.

## Example output from the show isakmp peer command

|                         |                        |          |
|-------------------------|------------------------|----------|
| awplus#show isakmp peer |                        |          |
| Peer                    | Profile (* incomplete) | Key      |
| -----                   |                        |          |
| 10.1.1.1                | default                | PSK, EAP |
| 10.1.5.1                | SECURE                 | PSK      |
| example.com             | LEGACY                 | EAP      |

**Related commands** [crypto isakmp peer](#)

**Command changes** Version 5.4.7-0.1: Parameter **hostname** added for DDNS feature.

# show isakmp profile

**Overview** Use this command to show ISAKMP default and custom profiles.

**Syntax** show [crypto] isakmp profile [<profile\_name>]

| Parameter      | Description          |
|----------------|----------------------|
| <profile_name> | Custom profile name. |

**Mode** Privileged Exec

**Examples** To show ISAKMP profiles, including the default profile, use the command:  
awplus# show isakmp profile

**Output** The following shows typical output.

## 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** The following shows typical output.

**Example output from the show isakmp profile my\_profile command**

```
awplus#show isakmp profile my_profile
ISAKMP Profile: my_profile
 Version: IKEv2
 Authentication: PSK
 Expiry: 24h
 DPD Interval: 30s
 Transforms:
 Integrity Encryption DH Group
 2 SHA1 3DES 5
```

**Related commands** [crypto isakmp profile](#)



# show isakmp sa

**Overview** Use this command to show current IKE security associations at a peer.

**Syntax** show [crypto] isakmp sa

| Parameter | Description                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------|
| crypto    | Security specific command.                                                                                            |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| sa        | Security Association.                                                                                                 |

**Mode** Privileged Exec

**Examples** To show current IKE security associations at a peer, enter the command below:

```
awplus# show isakmp sa
```

**Output** The following shows typical output.

## Example output from the show isakmp sa command

|                       |                                   |           |       |      |      |             |
|-----------------------|-----------------------------------|-----------|-------|------|------|-------------|
| awplus#show isakmp sa |                                   |           |       |      |      |             |
| Peer                  | Cookies (initiator:responder)     |           |       | Auth | Ver  | Expires     |
|                       | Encryption                        | Integrity | Group | DPD  | NATT | State       |
| 10.0.0.20             | f93c2717a1ece407:972bc0c77344d7a4 |           |       | PSK  | 1    | 78340s      |
|                       | AES256                            | SHA256    | 2     | yes  | no   | Established |
| 10.0.0.22             | ccb7f90b54945375:2642525bd20f3428 |           |       | PSK  | 1    | 3334s       |
|                       | 3DES                              | SHA1      | 2     | yes  | no   | Established |
| 10.0.0.25             | bd0efef134c86656:d46d0b1b72b46444 |           |       | PSK  | 1    | 819s        |
|                       | AES128                            | SHA1      | 2     | yes  | no   | Established |

# show tunnel inline-processing counters

**Overview** Use this command to show the tunnel inline-processing counters.

**Syntax** show tunnel inline-processing counters

**Mode** Privileged Exec

**Usage notes** Global counters show packet counts (esp, frames, nsh, oam), packet decisions (decrypts, drops), and IPsec SAs tracked by tunnel inline (msg\_...,sa\_added, sa\_deleted).

Per worker counters show the packet counts and decisions made by each worker and activity counters (fetch, sleep, wakeup,...).

**Example** To display tunnel inline-processing counters, use the command:

```
awplus# show tunnel inline-processing counters
```

**Output** The following shows typical output.

**Example output from show tunnel inline-processing counters**

```
show tunnel inline-processing counters
Global Counters:
 decrypts 4913089
 drop 0
 err_not_esp 0
 err_trans_auth 0
 err_trans_crypto 0
 esp 4913089
 esp_error_internal 0
 esp_error_invalid_hmac 0
 esp_error_malformed 0
 esp_error_replay_fail 0
 esp_no_sa 0
 espinudp 0
 frames 7518246
 ignore 2605157
 msg_del_sa 0
 msg_expired_sa 0
 msg_flush_sa 0
 msg_new_sa 0
 msg_unknown 0
 msg_updated_sa 0
 nsh 7518246
 oam 0
 sa_added 2
 sa_deleted 0...

worker0: sleeping
 decrypts 1386914
 drop 0
 esp 1386914
 esp_error_internal 0
 esp_error_invalid_hmac 0
 esp_error_malformed 0
 esp_error_replay_fail 0
 esp_no_sa 0
 espinudp 0
 fetch00 617322
 fetch01 407403
 fetch02_03 155630
 fetch04_07 36150
 fetch08_15 11152
 fetch16_31 2457
 fetch32_63 2553
 fetch64_ 2787
 frames 2669292
 ignore 1282378
 nsh 2669292
 oam 0
 return00 0
 return01 407403
 return02_03 155630
 return04_07 36150
 return08_15 11152
 return16_31 2457
 return32_63 2553
 return64_ 2787
 sleep 617322
 sleep_cmd 617322
 sleep_user 0
 sleep_work 617322
 wakeup 617321
 wakeup_cmd 0
 wakeup_user 0
 wakeup_work 617321
```

**Related** [tunnel inline-processing](#)  
**commands**

**Command** Version 5.5.2-1.1: command added  
**changes**

## transform (IPsec Profile)

**Overview** Use this command to create an IPsec profile transform, which specifies the encryption and authentication algorithms used to protect data.

Use the **no** variant to delete a previously created transform.

**Syntax**

```
transform <1-255> protocol esp integrity {sha1|sha256|sha512}
 encryption {3des|aes128|aes192|aes256|null}
transform <1-255> protocol esp integrity {gcm8|gcm12|gcm16}
 encryption {aes128|aes192|aes256}
no transform <1-255>
```

| Parameter | Description                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| <1-255>   | Transform priority (1 is the highest).                                                                             |
| sha1      | Secure Hash Standard with 160-bit digest size.                                                                     |
| sha256    | Secure Hash Standard with 256-bit digest size.                                                                     |
| sha512    | Secure Hash Standard with 512 bit digest size.                                                                     |
| 3des      | Triple DES symmetric key block cipher with a 168-bit key.                                                          |
| aes128    | Advanced Encryption Standard symmetric key block cipher with a 128-bit key.                                        |
| aes192    | Advanced Encryption Standard symmetric key block cipher with a 192-bit key.                                        |
| aes256    | Advanced Encryption Standard symmetric key block cipher with a 256-bit key.                                        |
| gcm8      | Galois/Counter Mode that uses an 8-byte authentication tag.                                                        |
| gcm12     | Galois/Counter Mode that uses a 12 byte authentication tag.                                                        |
| gcm16     | Galois/Counter Mode that uses a 16 byte authentication tag.                                                        |
| null      | No encryption. This option is not intended for use in a live network. It should only be used for testing purposes. |

**Default** By default, an IPsec profile has no transforms and so will not be active.

**Mode** IPsec Profile Configuration

**Examples** To configure an IPsec profile transform, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
```

```
awplus(config-ipsec-profile)# transform 2 protocol esp integrity
sha1 encryption 3des
```

To delete a created transform, use the following command:

```
awplus(config-ipsec-profile)# no transform 2
```

**Related commands** [crypto ipsec profile](#)

**Validation Commands** [show ipsec profile](#)

**Command changes** Version 5.5.3-2.1: **gcm** parameters added

## transform (ISAKMP Profile)

**Overview** Use this command to create an ISAKMP profile transform which specifies the encryption and authentication algorithms used to protect data in the tunnel.

Use the **no** variant to delete a previously created transform.

**Syntax** transform <1-255> integrity {sha1|sha256|sha512} encryption {3des|aes128|aes192|aes256} group {2|5|14|15|16|18}  
no transform <1-255>

| Parameter | Description                                                                |
|-----------|----------------------------------------------------------------------------|
| <1-255>   | Transform priority (1 is the highest)                                      |
| sha1      | Secure Hash Standard with 160-bit digest size                              |
| sha256    | Secure Hash Standard with 256-bit digest size                              |
| sha512    | Secure Hash Standard with 512 bit digest size                              |
| 3des      | Triple DES symmetric key block cipher with a 168-bit key                   |
| aes128    | Advanced Encryption Standard symmetric key block cipher with a 128-bit key |
| aes192    | Advanced Encryption Standard symmetric key block cipher with a 192-bit key |
| aes256    | Advanced Encryption Standard symmetric key block cipher with a 256-bit key |
| group     | Diffie-Hellman group                                                       |
| 2         | 1024-bit MODP Group                                                        |
| 5         | 1536-bit MODP Group                                                        |
| 14        | 2048-bit MODP Group                                                        |
| 15        | 3072-bit MODP Group                                                        |
| 16        | 4096-bit MODP Group                                                        |
| 18        | 8192-bit MODP Group                                                        |

**Default** By default, an ISASMP profile has no transforms and so will not be active.

**Mode** ISAKMP Profile Configuration

**Examples** To create an ISAKMP profile transform, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a created transform, use the following command:

```
awplus(config-isakmp-profile)# no transform 2
```

**Related commands** [crypto isakmp profile](#)



## tunnel destination (IPsec)

**Overview** Use this command to specify a destination IPv4 or IPv6 address or destination network name for the remote end of the tunnel.

Use the **no** variant of this command to remove a configured tunnel destination address.

**Syntax** tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}  
no tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}

| Parameter      | Description                                                                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD>         | Destination network name or “dynamic”. The “dynamic” parameter allows you to specify a dynamic IP address for the remote endpoint. The dynamic IP address can be obtained, for example, via DHCP. |
| <ipv4-address> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.                                                                                                                               |
| <ipv6-address> | Destination IPv6 address. The IPv6 address uses the format X:X::X:X.                                                                                                                              |

**Mode** Interface Configuration

**Examples** To configure a destination IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination 192.0.3.1
```

To configure a destination IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel destination 2001:0db8::
```

To configure a destination network name for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination www.example.com
```

To configure a dynamic IP address for the tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination dynamic
```

To remove the destination address of IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel destination 192.0.3.1
```

**Related commands** [tunnel source \(IPsec\)](#)

# tunnel inline-processing

**Overview** Use this command to configure tunnel inline-processing for an IPsec encrypted tunnel.

Tunnel inline-processing is a faster alternative to tunnel security-reprocessing which is the alternative, less efficient option. With tunnel security-reprocessing configured, the DPI engine processes incoming VPN traffic twice (before and after decryption), in order to identify incoming application traffic transported via an encrypted VPN.

Tunnel inline-processing is useful because it means packets are decrypted before being analysed and processed via the DPI engine. This is especially important for VPN traffic, where you actually want to identify application traffic transported within the IPsec VPN, rather than the outer encrypted IPsec VPN headers.

Use the **no** variant of this command to disable tunnel inline-processing for an IPsec encrypted tunnel.

**Syntax** tunnel inline-processing  
no tunnel inline-processing

**Default** Disabled

**Mode** Interface Configuration

**Example** To enable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel inline-processing
```

To disable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel inline-processing
```

**Related commands** [show tunnel inline-processing counters](#)

**Command changes** Version 5.5.2-1.1: command added

# tunnel local name (IPsec)

**Overview** Use this command to specify an IPsec tunnel hostname to send to the peer for authentication when you apply **tunnel protection ipsec (IPsec)** to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured IPsec tunnel hostname.

**Syntax** tunnel local name *<local-name>*  
no tunnel local name

| Parameter                 | Description             |
|---------------------------|-------------------------|
| <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                          | Descripti                                                            |
|------------------------------------|----------------------------------------------------------------------|
| <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:

```
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:

```
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 oper-status-control

**Overview** Use this command to configure the control of operation status for point-to-point IPsec protected tunnels. This type of tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN'.

Use the **no** variant of this command to return a tunnel to the default configuration of not using the existence of an IPsec SA to set the oper-status of the tunnel.

**Syntax** tunnel oper-status-control {ipsec|none}  
no tunnel oper-status-control

| Parameter | Description                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| ipsec     | Use the presence or absence of an IPsec SA, associated with an IPsec-protected tunnel to control the oper-status of the tunnel interface. |
| none      | Always show the oper-status of the tunnel as 'Link is UP' and 'RUNNING'.                                                                  |

**Default** None.

**Mode** Interface Configuration

**Usage notes** By default, when a tunnel is fully configured and is administratively enabled, the tunnel always shows 'Link is UP' and the RUNNING flag is always set in the output of the **show interface** command. This is because tunnels are virtual interfaces that have no electrical state associated with them. However, this does not mean that the tunnel is capable of passing traffic.

In order to provide a kind of oper-status for point-to-point IPsec protected tunnels, the tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN', respectively. When configured in this way the device will always attempt to maintain an IPsec SA with the remote device, whereas normally one would only be established if there is traffic that needs to be passed. This is necessary, otherwise routes over the tunnel would not be considered active.

**Example** To use the presence of IPsec SA's to control the oper-status of interface 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel oper-status-control ipsec
```



**Output 1** In this first example, there is an IPsec SA (i.e. IPsec has negotiated and is ready to send data) and so the link shows as 'UP'.

**Example output from show interface tunnel1**

```
awplus#show interface tunnel1
Interface tunnel1
 Link is UP, administrative state is UP
 Hardware is Tunnel
 IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
 index 17 metric 1 mtu 1438
 UP, POINT-TO-POINT, RUNNING, MULTICAST
 SNMP link-status traps: Disabled
 Bandwidth 1g
 Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
 Tunnel name local 172.16.1.1, remote 172.16.1.2
 Tunnel traffic selectors (ID, local, remote)
 1 0.0.0.0/0 0.0.0.0/0
 Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
 Checksumming of packets disabled, DF bit set, path MTU discovery disabled
 Tunnel protection via IPsec (profile "default")
 Router Advertisement is disabled
 Router Advertisement default routes are accepted
 Router Advertisement prefix info is accepted
 input packets 0, bytes 0, dropped 0, multicast packets
 output packets 0, bytes 0, multicast packets 0, broadcast packets 0
 input average rate : 30 seconds 0 bps, 5 minutes 0 bps
 output average rate: 30 seconds 0 bps, 5 minutes 0 bps
 Time since last state change: 0 days 00:00:49
 ...
```

**Output 2** In the second example there is no IPsec SA and so the link is 'DOWN'.

**Example output from show interface tunnel1**

```
awplus#show interface tunnel1
Interface tunnel1
 Link is DOWN, administrative state is UP
 Hardware is Tunnel
 IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
 index 17 metric 1 mtu 1438
 UP, POINT-TO-POINT, MULTICAST
 SNMP link-status traps: Disabled
 Bandwidth 1g
 Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
 Tunnel name local 172.16.1.1, remote 172.16.1.2
 Tunnel traffic selectors (ID, local, remote)
 1 0.0.0.0/0 0.0.0.0/0
 Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
 Checksumming of packets disabled, DF bit set, path MTU discovery disabled
 Tunnel protection via IPsec (profile "default")
 Router Advertisement is disabled
 Router Advertisement default routes are accepted
 Router Advertisement prefix info is accepted
 input packets 0, bytes 0, dropped 0, multicast packets
 output packets 0, bytes 0, multicast packets 0, broadcast packets 0
 input average rate : 30 seconds 0 bps, 5 minutes 0 bps
 output average rate: 30 seconds 0 bps, 5 minutes 0 bps
 Time since last state change: 0 days 00:00:49
 ...
```

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

**Command changes** Version 5.5.1-2.1: command added

# tunnel protection ipsec (IPsec)

**Overview** Use this command to enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

**Syntax** tunnel protection ipsec [profile <profile\_name>]  
no tunnel protection ipsec

**Default** IPsec protection for packets encapsulated by tunnel is disabled. If no custom profile is specified, the default profile is used.

| Parameter      | Description                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------|
| <profile_name> | Custom profile name. You can use the <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                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------|
| <traffic-selector-ID> | Traffic selector ID from 1 through 65535. If not specified the default value 1 is used. |
| <ipv4-subnet>         | IPv4 subnet in the format A.B.C.D/M.                                                    |
| <ipv6-subnet>         | IPv6 subnet in the format of X:X::X:X/M                                                 |

**Default** When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

**Mode** Interface configuration

**Usage notes** A traffic selector pair is an agreement between IKE peers to permit 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:

```
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:

```
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-name> | Interface name.                            |
| <ipv4-address>   | The IPv4 address uses the format A.B.C.D.  |
| <ipv6-address>   | The IPv6 address uses the format X:X::X:X. |

**Mode** Interface Configuration

**Examples** To configure a source IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source 192.168.1.1
```

To configure a source IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel source 2001:db8::
```

To configure a source interface for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source eth1
```

To remove the source address of IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel source 192.168.1.1
```

**Related** [tunnel destination \(IPsec\)](#)  
**commands**

# 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](#)

# 49 GRE Tunneling Commands

- Contents**
- **Introduction** on page 2283
  - **interface tunnel (GRE)** on page 2284
  - **show interface tunnel (GRE)** on page 2285
  - **tunnel checksum** on page 2286
  - **tunnel dscp** on page 2287
  - **tunnel destination (GRE)** on page 2288
  - **tunnel local name (GRE)** on page 2290
  - **tunnel mode gre** on page 2291
  - **tunnel protection ipsec (GRE)** on page 2292
  - **tunnel remote name (GRE)** on page 2293
  - **tunnel security-reprocessing** on page 2294
  - **tunnel source (GRE)** on page 2295
  - **tunnel ttl** on page 2297

# Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure IPv6 tunnels. For more information about IPv6 tunnels, see the **Generic Routing Encapsulation (GRE) Feature Overview and Configuration Guide**.

# interface tunnel (GRE)

**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 through 65535. |

**Default** Tunnel interfaces do not exist.

**Mode** Global Configuration

**Usage notes** After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

**Examples** To configure a tunnel interface with index 30 and enable GRE, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode gre
```

To remove the GRE tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

**Command changes** Version 5.4.7-2.1: increased range for **tunnel** index identifiers.



# show interface tunnel (GRE)

**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 <0-65535> parameter. |
| <0-65535> | Specify a tunnel index in the range from 0 through 65535.                                                            |

**Mode** Privileged Exec

**Example** To display status information for GRE tunnel tunnel20, use the command:

```
awplus# show interface tunnel20
```

## Example output from the show interface tunnel command

```
awplus#show interface tunnel20
Interface tunnel20
 Link is UP, administrative state is UP
 Hardware is Tunnel
 IPv4 address 172.16.1.1/24 pointopoint 172.16.1.255
 index 4750 metric 1 mtu 1480
 arp ageing timeout 300
 <UP,POINTOPOINT,RUNNING,MULTICAST>
 SNMP link-status traps: Disabled
 Tunnel source 192.168.1.1, destination 192.168.2.1
 Tunnel local 192.168.1.1, remote 192.168.2.1
 Tunnel protocol/transport gre, key disabled, sequencing
 disabled
 Tunnel TTL inherit
 Checksumming of packets disabled, path MTU discovery disabled
 input packets 0, bytes 0, dropped 0, multicast packets 0
 output packets 0, bytes 0, multicast packets 0 broadcast
 packets 0
 Time since last state change: 0 days 00:05:25
```

# tunnel checksum

**Overview** Use this command to enable GRE tunnel checksum insertion and checking. This results in the first two bytes after the protocol field in the IPv4 header containing the checksum. The tunnel checksum is used to detect packet corruption.

Use the **no** variant of this command to disable checksum insertion and checking.

**Syntax** tunnel checksum  
no tunnel checksum

**Default** Checksum insertion and checking is disabled.

**Mode** Interface Configuration

**Examples** To enable checksum insertion and checking, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel checksum
```

To disable checksum insertion and checking, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel checksum
```

## 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 destination (GRE)

**Overview** Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv4 address.

Use the **no** variant of this command to remove a configured tunnel destination.

**Syntax** tunnel destination {<ipv4-addr>|<destination-network-name>}  
no tunnel destination

| Parameter                  | Description                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-addr>                | Specify the tunnel destination IPv4 address in the dotted decimal format A.B.C.D.<br><br>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.<br><br>If the destination network name cannot be resolved, then the GRE tunnel remains inactive.                                                                                                                                                       |

**Mode** Interface Configuration

**Examples** To configure an IPv4 tunnel destination by using an IPv4 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel destination 2.2.2.2
```

To configure a GRE tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel destination corporate_lan.example.com
```

To remove a GRE tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

**Related** **interface tunnel (GRE)**  
**commands** **tunnel mode gre**  
**tunnel source (GRE)**

## tunnel local name (GRE)

**Overview** Use this command to specify an IPsec tunnel hostname to send to the peer for authentication when you apply **tunnel protection ipsec (GRE)** 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 (GRE)**

## tunnel mode gre

**Overview** Use this command to configure the encapsulation tunneling mode to use. This command sets GRE IPv4 or IPv6 as the payload over IPv4 or IPv6 tunneling.

Use the **no** variant of this command to remove an established tunnel.

**Syntax** tunnel mode gre [ipv6]  
no tunnel mode

| Parameter | Description                                                                                 |
|-----------|---------------------------------------------------------------------------------------------|
| gre ipv6  | Specify GRE IPv4 or IPv6 as the payload over IPv6 tunneling. IPv6 is the delivery protocol. |

**Default** Virtual tunnel interfaces have no mode set by default. If you specify a mode of **gre**, the delivery protocol is IPv4 unless you specify IPv6.

**Mode** Interface Configuration

**Usage notes** A tunnel will not become operational until it is configured with this command.

**Examples** To configure GRE as the encapsulation mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
```

To remove a configured GRE tunnel mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel mode
```

**Related commands** [interface tunnel \(GRE\)](#)

# tunnel protection ipsec (GRE)

**Overview** Use this command to optionally enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

**Syntax** tunnel protection ipsec [profile <ipsec-profile>]  
no tunnel protection ipsec

| Parameter       | Description                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------|
| <ipsec-profile> | The name of an optional custom IPsec profile ( <b>crypto ipsec profile</b> command) to use to protect this tunnel. |

**Default** IPsec protection for packets encapsulated by tunnel is disabled.

**Mode** Interface Configuration

**Usage notes** You also need to configure a pre-shared key in conjunction with this command. See the **crypto isakmp key** for more information about configuring the pre-shared key.

**Examples** To enable IPsec protection for packets encapsulated by tunnel14, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To disable IPsec protection for packets encapsulated by tunnel14, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

**Related commands** **crypto ipsec profile**  
**crypto isakmp key**  
**show isakmp key (IPsec)**



# tunnel remote name (GRE)

**Overview** Use this command to specify a tunnel remote name to authenticate the tunnel's remote peer device when you apply **tunnel protection ipsec (GRE)** 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 (GRE)**

# tunnel security-reprocessing

**Overview** Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

**Syntax** tunnel security-reprocessing  
no tunnel security-reprocessing

**Default** Security reprocessing is disabled by default.

**Mode** Global Configuration

**Usage notes** Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and\\_Configuration Guide](#).

**Example** To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

**Related commands** [show interface tunnel \(IPsec\)](#)

**Command changes** Version 5.4.8-0.2: command added

## tunnel source (GRE)

**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 IPv4 address. The source address must be an existing IPv4 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

**Syntax** `tunnel source {<ipv4-addr>|<interface-name>}`  
`no tunnel source`

| Parameter                           | Description                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code>      | <p>Specify the tunnel source IPv4 address for the GRE tunnel interface in the dotted decimal format A.B.C.D.</p> <p>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.</p> |
| <code>&lt;interface-name&gt;</code> | <p>Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc).</p> <p>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.</p>                                    |

**Mode** Interface Configuration

**Examples** To configure a GRE tunnel source IPv4 address, use the commands:

```
awplus# configure terminal
awplus# interface eth1
awplus(config-if)# ip address 1.1.1.1/24
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel source 1.1.1.1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel source eth2
```

To remove a GRE tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

**Related commands** **interface tunnel (GRE)**  
**tunnel destination (GRE)**  
**tunnel mode gre**

## 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 \(IPv6\)](#)

# 50

## OpenVPN Commands

- Contents**
- **Introduction** on page 2299
  - **ip tcp adjust-mss** on page 2300
  - **ipv6 tcp adjust-mss** on page 2302
  - **show interface tunnel (OpenVPN)** on page 2304
  - **show openvpn connections** on page 2305
  - **show openvpn connections detail** on page 2306
  - **tunnel mode openvpn tap** on page 2307
  - **tunnel mode openvpn tun** on page 2308
  - **tunnel openvpn authentication** on page 2309
  - **tunnel openvpn cipher** on page 2310
  - **tunnel openvpn expiry-bytes** on page 2312
  - **tunnel openvpn expiry-seconds** on page 2313
  - **tunnel openvpn port** on page 2314
  - **tunnel openvpn route** on page 2315
  - **tunnel openvpn tagging** on page 2317
  - **tunnel openvpn tls-crypt** on page 2318
  - **tunnel openvpn tls-version-min** on page 2319
  - **tunnel openvpn verify-client-certificate trustpoint** on page 2320
  - **tunnel openvpn verify-client-certificate strict-common-name-check** on page 2322
  - **tunnel security-reprocessing** on page 2324

# Introduction

This chapter provides an alphabetical reference of commands used to configure AlliedWare Plus OpenVPN.

For introductory information about AlliedWare Plus OpenVPN, including overview and configuration information, see the [OpenVPN Feature Overview and Configuration Guide](#).

The table below lists the OpenVPN commands and their applicable modes.

## OpenVPN commands and applicable modes

| Mode                    | Command                                         |
|-------------------------|-------------------------------------------------|
| Privileged Exec         | <a href="#">show openvpn connections</a>        |
|                         | <a href="#">show openvpn connections detail</a> |
| Interface Configuration | <a href="#">tunnel mode openvpn tap</a>         |
|                         | <a href="#">tunnel mode openvpn tun</a>         |
|                         | <a href="#">tunnel openvpn port</a>             |
|                         | <a href="#">tunnel openvpn tagging</a>          |

## 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                                                            |
|------------|------------------------------------------------------------------------|
| <mss-size> | <64-1460> Specifies the MSS size in bytes.                             |
| pmtu       | 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



**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                                                            |
|------------|------------------------------------------------------------------------|
| <mss-size> | <64-1460> Specifies the MSS size in bytes.                             |
| pmtu       | 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.

**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

# show interface tunnel (OpenVPN)

**Overview** Use this command to display status information of a tunnel.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

**Syntax** show interface tunnel<*tunnel-index*>

| Parameter               | Description                                    |
|-------------------------|------------------------------------------------|
| < <i>tunnel-index</i> > | The tunnel index in the range from 0 to 65535. |

**Mode** Privileged Exec

**Examples** To display brief status information for OpenVPN tunnel0, enter the command below:

```
awplus# show interface tunnel0
```

**Output** The following shows typical output.

## Example output from the show interface tunnel command

```
awplus#show interface tunnel0
Interface tunnel0
Link is UP, administrative state is UP
Hardware is Tunnel
IPv4 address 10.8.1.2/24 broadcast 10.8.1.255
IPv6 address fc00:5::2/64
IPv6 address fe80::5054:98ff:fe43:428e/64
index 22 metric 1 mtu 1405
<UP,BROADCAST,RUNNING,MULTICAST>
SNMP link-status traps: Disabled
Bandwidth 1g
Tunnel protocol/transport openvpn tap, listen port 1194
cipher aes128, authentication sha1
expiry-kbytes 0, expiry-seconds 3600
tls-version-min 1.0
Checksumming of packets disabled, DF bit set, path MTU discovery 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 6, bytes 452, multicast packets 0, broadcast packets 0
input average rate : 30 seconds 0 bps, 5 minutes 0 bps
output average rate: 30 seconds 73 bps, 5 minutes 11 bps
output peak rate 482 bps at 2021/03/08 01:29:01
Time since last state change: 0 days 00:00:41
```

**Command changes** Version 5.5.0-2.1: command added to AR1050V

# show openvpn connections

**Overview** Use this command to show information about connected OpenVPN users.

**Syntax** show openvpn connections

**Mode** Privileged Exec

**Examples** To show information about connected OpenVPN users, use the command:

```
awplus# show openvpn connections
```

**Output** The following shows typical output.

## Example output from the show openvpn connections command

```
awplus#show openvpn connections
Maximum connections: 100
Interface: tunnel0
Username Real Address Rx Tx Connected Since
Bytes Bytes

foo ::ffff:192.168.1.2 3553 3906 Wed Aug 13 01:09:07 2014
```

**Related commands** [show openvpn connections detail](#)

**Command changes** Version 5.5.0-2.1: command added to AR1050V

# show openvpn connections detail

**Overview** Use this command to show detailed information about connected OpenVPN users.

Note that in the output, parameters (such as Route, Address, DNS Server) for a specific user may vary because the parameters depend on the configuration information of the RADIUS server associated with the user.

**Syntax** show openvpn connections detail

**Mode** Privileged Exec

**Examples** To show detailed information about connected OpenVPN users, use the command:

```
awplus# show openvpn connections detail
```

**Output** The following shows typical output.

## Example output from the show openvpn connections detail command

```
awplus#show openvpn connections detail

Interface: tunnel0
Username: user1
 Route: 192.168.20.0 255.255.255.0 192.168.10.2
 Address: 192.168.10.3 255.255.255.0
 DNS Server: 192.168.10.253
 DNS Server: 192.168.10.254
 VID: 20
Username: user2
 Route: 192.168.20.0 255.255.255.0 192.168.10.2
 Address: 192.168.10.4 255.255.255.0
 DNS Server: 192.168.10.253
 DNS Server: 192.168.10.254
 VID: 20
```

**Related commands** [show openvpn connections](#)

**Command changes** Version 5.5.0-2.1: command added to AR1050V

# tunnel mode openvpn tap

**Overview** Use this command to set the tunnel mode to OpenVPN TAP for a tunnel interface.

Use the **no** variant of this command to remove the mode.

TAP is a virtual network device. TAP creates a Virtual Tunnel Interface (VTI) that carries layer 2 frames. You may want to use TAP in the following scenarios:

- You want to use bridges to transport Ethernet frames
- You want to transport any network protocol, such as IPv4, IPv6, IPX

Note that TAP will cause broadcast overhead on the VPN tunnel and add the overhead of Ethernet headers on all packets transported over the VPN tunnel.

Note that the distribution of client IP addresses through DHCP is only supported in TAP mode.

**Syntax** tunnel mode openvpn tap  
no tunnel mode

**Mode** Interface Configuration

**Examples** To set tunnel5 to be an OpenVPN tunnel in TAP mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel mode openvpn tap
```

To remove the configured mode for tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel mode
```

**Related commands** [tunnel mode openvpn tun](#)

**Command changes** Version 5.5.0-2.1: command added to AR1050V

# tunnel mode openvpn tun

**Overview** Use this command to set the tunnel mode to OpenVPN TUN for a tunnel interface.

Use the **no** variant of this command to remove the mode.

TUN is a virtual network device. TUN creates a Virtual Tunnel Interface (VTI) that carries layer 3 packets. You may want to use TUN in the following scenarios:

- You want to transport traffic that is destined for the VPN client
- You want to transport only layer 3 packets
- You want to support VPN on mobile devices

Note that TUN cannot be used in bridges and broadcast traffic is not transported in TUN mode.

**Syntax** tunnel mode openvpn tun  
no tunnel mode

**Mode** Interface Configuration

**Examples** To set tunnel5 to be an OpenVPN tunnel in TUN mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel mode openvpn tun
```

To remove the configured mode for tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel mode
```

**Related commands** [tunnel mode openvpn tap](#)

**Command changes** Version 5.5.0-2.1: command added to AR1050V



# tunnel openvpn authentication

**Overview** Use this command to configure the data channel authentication digest for an OpenVPN tunnel.

Use the **no** variant of this command to set the data channel authentication digest for an OpenVPN tunnel to its default value of SHA1.

**Syntax** tunnel openvpn authentication {sha1|sha256}  
no tunnel openvpn authentication

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| sha1      | Use Secure Hash Standard with 160-bit digest size as the data channel authentication digest. |
| sha256    | Use Secure Hash Standard with 256-bit digest size as the data channel authentication digest. |

**Default** SHA1

**Mode** Interface configuration

**Usage notes** You need to configure the client to use the same setting as the server. To do this, include one of the following lines in your client's OpenVPN configuration (.ovpn) file:

| Setting | Line        |
|---------|-------------|
| SHA1    | auth SHA1   |
| SHA256  | auth SHA256 |

**Example** To configure tunnel 5, which is an OpenVPN tunnel, to use SHA256 data channel authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn authentication SHA256
```

**Related commands** [tunnel openvpn cipher](#)  
**Command changes** Version 5.4.7-0.1: command added  
Version 5.5.0-2.1: command added to AR1050V

## tunnel openvpn cipher

**Overview** Use this command to configure the data channel encryption cipher for an OpenVPN tunnel.

Use the **no** variant of this command to set the data channel encryption cipher for an OpenVPN tunnel to its default value of AES-128.

**Syntax** tunnel openvpn cipher {aes128|aes256}  
no tunnel openvpn cipher

| Parameter | Description                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------|
| aes128    | Use Advanced Encryption Standard symmetric key block cipher with a 128-bit key as the data channel encryption cipher. |
| aes256    | Use Advanced Encryption Standard symmetric key block cipher with a 256-bit key as the data channel encryption cipher. |

**Default** AES-128

**Mode** Interface configuration

**Usage notes** You need to configure the client to use the same setting as the server. To do this, include one of the following lines in your client's OpenVPN configuration (.ovpn) file:

| Setting | Line               |
|---------|--------------------|
| AES-128 | cipher AES-128-CBC |
| AES-256 | cipher AES-256-CBC |

For example, consider a client file tun.ovpn that has the following settings:

```
tun.ovpn
client
auth-user-pass
cipher AES-128-CBC
dev tap
proto udp
remote 192.168.1.1
ca c:/users/support/cacert.pem
verb 7
```

To change the client to AES-256, replace the line "cipher AES-128-CBC" with "cipher AES-256-CBC".

**Example** To configure tunnel 5, which is an OpenVPN tunnel, to use AES-256 data channel encryption, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn cipher aes256
```

**Related commands** [tunnel openvpn authentication](#)

**Command changes** Version 5.4.7-0.1: command added

Version 5.5.0-2.1: command added to AR1050V

# tunnel openvpn expiry-bytes

**Overview** Use this command to change how the firewall decides when to renegotiate client keys. By default, client keys are renegotiated after an hour; you can use this command to base rekeying on data usage instead of time.

Use the **no** variant of this command to return to time-based rekeying instead.

**Syntax** tunnel openvpn expiry-bytes <0-4294967295>  
no tunnel openvpn expiry-bytes

| Parameter                      | Description                                                                                                                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| expiry-bytes<br><0-4294967295> | The number of bytes of traffic after which the firewall renegotiates client keys. A value of 0 bytes means that keys are not renegotiated after the VPN is formed. Otherwise, setting the expiry-bytes to a non-zero value will cause a rekey when the firewall has received that many bytes of traffic. |

**Default** Not configured - the firewall renegotiates keys every hour instead.

**Mode** Interface mode for a tunnel

**Example** To configure tunnel2 to rekey after 1 GB of traffic, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn expiry-bytes 1000000000
```

To return tunnel2 to the default of rekeying hourly, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel openvpn expiry-bytes
```

**Related commands** [tunnel openvpn expiry-seconds](#)

**Command changes** Version 5.4.7-0.1: command added  
Version 5.5.0-2.1: command added to AR1050V

# tunnel openvpn expiry-seconds

**Overview** Use this command to change when client keys are renegotiated. By default, client keys are renegotiated after an hour; you can use this command to turn off renegotiation or to change that time period.

Use the **no** variant of this command to return to the default of 1 hour.

**Syntax** tunnel openvpn expiry-seconds <0-4294967295>  
no tunnel openvpn expiry-seconds

| Parameter                        | Description                                                                                                                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| expiry-seconds<br><0-4294967295> | The length of time after which the firewall renegotiates client keys. A value of 0 seconds means that keys are not renegotiated after the VPN is formed. Otherwise, setting the expiry-seconds to a non-zero timer value will cause a rekey when that time is exceeded. |

**Default** 3600 seconds (1 hour).

**Mode** Interface mode for a tunnel

**Example** To configure tunnel2 to rekey every 30 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn expiry-seconds 1800
```

To return tunnel2 to the default of rekeying hourly, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel openvpn expiry-seconds
```

**Related commands** [tunnel openvpn expiry-bytes](#)

**Command changes** Version 5.4.7-0.1: command added  
Version 5.5.0-2.1: command added to AR1050V

# tunnel openvpn port

**Overview** Use this command to specify the UDP listening port that is used to receive OpenVPN tunnel connections.

Use the **no** variant to set the port number to its default value which is 1194.

**Syntax** tunnel openvpn port <1-65535>  
no tunnel openvpn port

| Parameter | Description                       |
|-----------|-----------------------------------|
| <1-65535> | Port number from 1 through 65535. |

**Default** The default UDP port number is 1194.

**Mode** Interface Configuration

**Usage notes** If firewall protection is enabled, you need to create a firewall rule that allows the OpenVPN application traffic to traverse the firewall. OpenVPN is a pre-defined application with destination port number 1194. You can use the **show application detail** command to see the application details. If you specify a UDP number that is different to the default port number, you need to create an application with the same specified UDP port number for OpenVPN, and then create a firewall rule to allow the application to traverse the firewall. For more information about firewall rules, see the **rule (firewall)** command.

**Examples** To configure tunnel tunnel5 to receive incoming tunnel connections on UDP port 4567, use the commands:

```
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn port 4567
```

To remove the specified UDP port for tunnel tunnel5 and set the UDP port to its default value, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel openvpn port
```

**Command changes** Version 5.5.0-2.1: command added to AR1050V

## tunnel openvpn route

**Overview** Use this command to push route information based on an entity as part of the OpenVPN client configuration.

When an OpenVPN client connects, the IPv4 and IPv6 host addresses and network subnets for that entity are pushed to the client. This ensures that the client routes those addresses and subnets through the OpenVPN tunnel to the AlliedWare Plus device.

Use the **no** variant of this command to stop pushing the entity as routes to OpenVPN clients.

**Syntax** tunnel openvpn route *<entity>*  
no tunnel openvpn route

| Parameter             | Description                                                                 |
|-----------------------|-----------------------------------------------------------------------------|
| <i>&lt;entity&gt;</i> | Name of entity containing subnets and addresses to be routed to the device. |

**Mode** Interface Configuration

- Usage notes**
- The gateway IP used will be a configured IP of the OpenVPN tunnel. Host addresses will be sent as /32 IPv4 routes or /128 IPv6 routes.
  - If the network subnets and host IPs change on the entity, client connections will not be automatically updated. Clients will need to reconnect to receive the new routes.
  - Entity network subnets with a configured interface will not be used, as the interface restriction is not applicable for the OpenVPN client in this context.

**Example** To set up a specific part of the network with certain IP ranges and addresses that will be sent to the OpenVPN client, and ensure that the OpenVPN client directs traffic for these IP ranges to the correct device, use the following commands.

```
awplus# configure terminal
awplus(config)# zone openvpn_routes
awplus(config-zone)# network internet
awplus(config-network)# host example
awplus(config-host)# ip address dynamic fqdn example.com
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# network local
awplus(config-network)# ip subnet 172.16.0.0/16
awplus(config-network)# host example
awplus(config-host)# ip address 10.255.0.1
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# exit
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn route openvpn_routes
```

To stop pushing an entity as routes to OpenVPN clients, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn route
```

**Related commands** [tunnel mode openvpn tap](#)  
[tunnel mode openvpn tun](#)

**Command changes** Version 5.5.4-0.1: command added



# tunnel openvpn tagging

**Overview** This command configures an OpenVPN tunnel to add an 802.1Q tag (a VLAN ID) to traffic received over the tunnel. VLAN ID (VID) is a VLAN identifier that is used to determine which VLAN the traffic belongs to. The VID is determined from information received from the RADIUS server during the authentication process. If no VID information is received from the RADIUS server, the value specified in this command is used.

Use the **no** variant of this command to remove the VID over the tunnel.

Note that you can add an 802.1Q tag in the TAP mode only.

**Syntax** tunnel openvpn tagging <1-4094>  
no tunnel openvpn tagging

| Parameter | Description                 |
|-----------|-----------------------------|
| <1-4094>  | VLAN ID from 1 through 4094 |

**Mode** Interface Configuration

**Examples** To add an 802.1Q tag of 1 to packets received over the tunnel named tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn tagging 1
```

To remove the 802.1Q tag for the tunnel named tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel openvpn tagging
```

**Command changes** Version 5.5.0-2.1: command added to AR1050V

# tunnel openvpn tls-crypt

**Overview** Use this command to enable TLS Crypt on OpenVPN. TLS Crypt uses a pre-shared key to secure the entire OpenVPN session from the first packet. It provides several potential benefits:

- It prevents detection of the OpenVPN connection start, which is helpful in some situations when the OpenVPN protocol signature is detected and blocked.
- It prevents TLS denial of service attacks. DoS attacks are possible with TLS-Auth, where the attacker can open thousands of TLS connections simultaneously but not provide a valid certificate, jamming the available ports. With TLS Crypt the server would reject the connection up front.
- Data is encrypted twice, once by TLS Crypt and once by the TLS session.

Use the **no** variant of this command to disable TLS Crypt.

**Syntax** tunnel openvpn tls-crypt <key-filename>  
no tunnel openvpn tls-crypt

| Parameter      | Description                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <key-filename> | The path to the key file that is shared with the clients. The filename starts with "flash:/" (e.g. flash:/openvpn.key). All clients and the server must share the same key file. TLS Crypt will automatically create the configured key file if it doesn't exist. |

**Default** Disabled

**Mode** Interface Configuration for a tunnel

**Example** To configure OpenVPN in TAP mode, and use the key file called 'openvpn.key' on tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn tls-crypt flash:/openvpn.key
awplus(config-if)# tunnel mode openvpn tap
```

**Related commands** [tunnel mode openvpn tap](#)  
[tunnel mode openvpn tun](#)

**Command changes** Version 5.5.2-0.1: command added

# tunnel openvpn tls-version-min

**Overview** Use this command to set the minimum TLS (Transport Layer Security) version allowed for OpenVPN.

Use the **no** variant of this command to revert to the default TLS version (1.0).

**Syntax** tunnel openvpn tls-version-min {1.1|1.2|1.3}  
no tunnel openvpn tls-version-min

| Parameter       | Description                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tls-version-min | Enter the minimum TLS version: 1.1, 1.2, or 1.3.<br><br>If the command is never entered, or the 'no' version is configured, then the default version 1.0 is used. |

**Default** 1.0

**Mode** Interface Configuration

**Example** To set the minimum TLS version as 1.1 on Open VPN tunnel1, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn tls-version-min 1.1
```

**Related commands** [tunnel openvpn cipher](#)  
[tunnel openvpn expiry-bytes](#)

**Command changes** Version 5.5.1-2.1: TLS version 1.3 added  
Version 5.5.1-0.1: command added

# tunnel openvpn verify-client-certificate trustpoint

**Overview** Use this command to enable OpenVPN to check a certificate provided by the client when they try to connect. This is a form of Two-Factor Authentication (2FA) called mutual trust. The certificate provided by the client, and the certificate owned by the server, must both be signed by the same certificate authority (CA).

Use the **no** variant of this command to disable the trustpoint.

**Syntax** `tunnel openvpn verify-client-certificate trustpoint <trustpoint-name>`  
`no tunnel openvpn verify-client-certificate trustpoint <trustpoint-name>`

| Parameter                            | Description                                                                                             |
|--------------------------------------|---------------------------------------------------------------------------------------------------------|
| <code>&lt;trustpoint-name&gt;</code> | The name of the trustpoint which contains the required certificates. For example, 'openvpn_selfsigned'. |

**Default** Disabled

**Mode** Interface Configuration

**Usage notes** The trustpoint part of the command allows the user to configure which certificates the server will be checking the client against. This is only available on the Interface Configuration for a tunnel.

**Examples** To enable this feature on 'tunnel1' and use the trustpoint called 'openvpn\_selfsigned', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn verify-client-certificate
trustpoint openvpn_selfsigned
```

To disable this feature on 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn verify-client-certificate
trustpoint openvpn_selfsigned
```

**Related commands** [tunnel openvpn verify-client-certificate strict-common-name-check](#)

**Command changes** Version 5.5.3-0.1: command added

# tunnel openvpn verify-client-certificate strict-common-name-check

**Overview** Use this command to provide a valid certificate and check that the common name on the certificate matches the client's username.

Use the **no** variant of this command to remove the strict common name check.

**Syntax** tunnel openvpn verify-client-certificate strict-common-name-check  
no tunnel openvpn verify-client-certificate strict-common-name-check

| Parameter                | Description                                                                     |
|--------------------------|---------------------------------------------------------------------------------|
| strict-common-name-check | The valid certificate common name. This name must match the client's user name. |

**Default** The strict common name check is enabled by default.

**Mode** Interface Configuration

**Usage notes** The strict common name check part of this command allows the user to provide a method for client certificate authentication for the OpenVPN server along with the username and password.

**Example** To disable this feature on 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn verify-client-certificate
strict-common-name-check
```

To require OpenVPN clients to provide a valid certificate and check that the common name on the certificate matches the client's username, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn verify-client-certificate
strict-common-name-check
```

**Output** The following shows typical output.

**Example output from tunnel openvpn verify-client-certificate**

```
awplus(config-if)#tunnel openvpn verify-client-certificate strict-
common-name-check

Strict name check is enabled
```

**Related commands** [tunnel openvpn verify-client-certificate trustpoint](#)

**Command changes** Version 5.5.3-0.1: 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



# 51

## L2TPv3 Ethernet Pseudowire Commands

- Contents**
- **Introduction** on page 2326
  - **interface tunnel (L2TPv3)** on page 2327
  - **l2tp unmanaged port** on page 2328
  - **show interface tunnel (L2TPv3)** on page 2329
  - **tunnel destination (L2TPv3)** on page 2330
  - **tunnel df** on page 2332
  - **tunnel local id** on page 2334
  - **tunnel mode l2tp v3** on page 2335
  - **tunnel protection ipsec** on page 2336
  - **tunnel remote id** on page 2337
  - **tunnel security-reprocessing** on page 2338
  - **tunnel source (L2TPv3)** on page 2339

# Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure L2TPv3 Ethernet pseudowires.

For introductory information about L2TPV3 in AlliedWare Plus, including overview and configuration information, see the [L2TPv3 Ethernet Pseudowire Feature Overview and Configuration Guide](#).

# interface tunnel (L2TPv3)

**Overview** Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

**Syntax** interface tunnel<0-65535>  
no interface tunnel<tunnel-index>

| Parameter | Description                                                                    |
|-----------|--------------------------------------------------------------------------------|
| <0-65535> | Specify a tunnel interface index identifier in the range from 0 through 65535. |

**Default** Tunnel interfaces do not exist.

**Mode** Global Configuration

**Usage notes** After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

**Examples** To configure a tunnel interface with index 30 and enable L2TPv3 mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode l2tp v3
```

To remove the tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

**Related commands** **show interface tunnel (L2TPv3)**  
**tunnel mode l2tp v3**

**Command changes** Version 5.4.7-2.1: increased range for **tunnel** index identifiers.

# l2tp unmanaged port

**Overview** Use this command to set the UDP port for an (IPv4 and IPv6) unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires).

This command can only change the UDP port when there is no unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires) configured.

Use the **no** variant of this command to reset the UDP port to the default (1701).

**Syntax** l2tp unmanaged port [<1-65535>]  
no l2tp unmanaged port

| Parameter | Description                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------|
| <1-65535> | The number of the UDP port to use for an unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires). |

**Default** The UDP port is 1701 by default.

**Mode** Global Configuration

**Usage notes** The default UDP port for both unmanaged and managed L2TP tunnels is 1701. If both kinds of tunnel will be configured, the UDP port for the unmanaged tunnel must be changed to a different port by using the **l2tp unmanaged port** command.

Be aware of potential clashes with other UDP port users. Unless it is likely to be used for other purposes, we recommend configuring UDP port 1702 as a suitable alternative.

**Example** To set the UDP port for an L2TP unmanaged tunnel (L2TPv3 Ethernet Pseudowires) to 1702, use the following commands:

```
awplus# configure terminal
awplus(config)# l2tp unmanaged port 1702
```

**Related commands** [tunnel mode l2tp v3](#)  
[show running-config](#)

# show interface tunnel (L2TPv3)

**Overview** Use this command to display status information of a tunnel.

**Syntax** show interface tunnel<0-65535>

| Parameter | Description                                               |
|-----------|-----------------------------------------------------------|
| <0-65535> | Specify a tunnel index in the range from 0 through 65535. |

**Mode** Privileged Exec

**Examples** To display status information for L2TPv3 tunnel tunnel20, use the command.

```
awplus#show interface tunnel20
```

**Output** The following shows typical output.

**Example output from show tunnel interface on the console.**

```
awplus#show interface tunnel20
Interface tunnel20
Link is UP, administrative state is UP
Hardware is Tunnel
IPv4 address 192.168.10.1/24 broadcast 192.168.10.255
IPv6 address 2001:db8:10::1/64
IPv6 address fe80::5054:d4ff:fe84:d1aa/64
index 16795714 metric 1 mtu 1480
arp ageing timeout 300
<UP,BROADCAST,RUNNING,MULTICAST>
SNMP link-status traps: Disabled
Tunnel source 192.168.1.1, destination 192.168.1.2
Tunnel name local 192.168.1.1, remote 192.168.1.2
Tunnel ID local 66, remote 77
Tunnel protocol/transport l2tp v3, key disabled, sequencing
disabled
Tunnel TTL inherit
Checksumming of packets disabled, path MTU discovery disabled

input packets 0, bytes 0, dropped 0, multicast packets 0
output packets 5, bytes 366, multicast packets 0 broadcast
packets 0
Time since last state change: 0 days 00:00:24
```

**Related** [interface tunnel \(L2TPv3\)](#)  
**commands**

## tunnel destination (L2TPv3)

**Overview** Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv4 address.

Use the **no** variant of this command to remove a configured tunnel destination.

**Syntax** tunnel destination {<ipv4-addr>|<destination-network-name>}  
no tunnel destination

| Parameter                  | Description                                                                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-addr>                | Specify the tunnel destination IPv4 address in the dotted decimal format A.B.C.D.<br><br>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.<br><br>If the destination network name cannot be resolved, then the L2TPv3 tunnel remains inactive.                                                                                                                                                    |

**Mode** Interface Configuration

**Examples** To configure an IPv4 tunnel destination by using an IPv4 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination 2.2.2.2
```

To configure an L2TPv3 tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination corporate_lan.example.com
```

To remove a tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

**Related** **interface tunnel (L2TPv3)**  
**commands** **tunnel mode l2tp v3**  
**tunnel source (L2TPv3)**

# tunnel df

**Overview** Use this command to specify whether the DF (Don't Fragment) bit in the IP header should be set or not on outgoing packets from L2TPv3 tunnels.

Use the **no** variant of this command to return to the default setting.

**Syntax** tunnel df {set|clear}  
no tunnel df

| Parameter | Description                          |
|-----------|--------------------------------------|
| set       | Set the DF bit in the outer header   |
| clear     | Clear the DF bit in the outer header |

**Default** The DF bit is **set** on all outgoing packets.

**Mode** Interface Configuration

**Usage notes** This command gives you the opportunity to clear the DF bit allowing packets greater than the MTU to be fragmented and transmitted via the L2TPv3 Ethernet pseudo-wire. This may be necessary if an L2TPv3 tunnel is connected to a bridge and MTU-exceeded messages cannot be sent back to clients.

**NOTE:** *If fragmentation of larger packets occurs as a result of setting the tunnel Do Not Fragment bit to clear, this may slightly increase latency of the associated traffic flow traversing the VPN, due to the fragmentation and re-assembly that occurs.*

**Example** To specify the DF bit on the L2TPv3 tunnel (tunnel2), use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel df clear
```

To set the DF bit on the L2TPv3 tunnel (tunnel2) back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel df
```

**Related commands** [tunnel mode l2tp v3](#)



**Command changes** Version 5.4.9-1.1: command added

# tunnel local id

**Overview** This command specifies a tunnel local identifier sent to the peer to match. Use the **no** variant of this command to remove the tunnel local ID.

**Syntax**

```
tunnel local id <1-2147483647>
no tunnel local id
```

| Parameter      | Description                         |
|----------------|-------------------------------------|
| <1-2147483647> | Tunnel ID from 1 through 2147483647 |

**Default** No tunnel local ID is set.

**Mode** Interface Configuration

**Usage notes** The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel local ID on one endpoint must be specified as the tunnel remote ID on the other endpoint.

The local session ID defaults to the tunnel local ID and the local session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

**Examples** To specify a tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel local id 22
```

To remove the tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel local id
```

**Related commands** [tunnel remote id](#)

**Validation Commands** [show interface tunnel \(L2TPv3\)](#)

# tunnel mode l2tp v3

**Overview** Use this command to configure the encapsulation tunneling mode.  
Use the **no** variant of this command to remove an established tunnel.

**Syntax** tunnel mode l2tp v3 [ipv6]  
no tunnel mode

| Parameter | Description                            |
|-----------|----------------------------------------|
| ipv6      | Specify IPv6 as the delivery protocol. |

**Default** Virtual tunnel interfaces have no mode set by default. If you specify a mode of **l2tp v3**, the delivery protocol is IPv4 unless you specify IPv6.

**Mode** Interface Configuration

**Usage notes** A tunnel will not become operational until it is configured with this command.

**Examples** To configure L2TPv3 as the encapsulation tunneling mode for tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
```

To remove the established tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel mode
```

**Related commands** **interface tunnel (L2TPv3)**  
**show interface tunnel (L2TPv3)**  
**tunnel df**

# tunnel protection ipsec

**Overview** Use this command to optionally enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant of this command to disable IPsec protection.

**Syntax** tunnel protection ipsec [profile <ipsec-profile>]  
no tunnel protection ipsec

| Parameter       | Description                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------|
| <ipsec-profile> | The name of an optional custom IPsec profile ( <b>crypto ipsec profile</b> command) to use to protect this tunnel. |

**Default** IPsec protection for packets encapsulated by tunnel is disabled.

**Mode** Interface Configuration

**Usage notes** You also need to configure a pre-shared key in conjunction with this command. See the **crypto isakmp key** command for more information about configuring the pre-shared key.

**Examples** To enable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#tunnel protection ipsec
```

To disable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#no tunnel protection ipsec
```

**Related commands** **crypto ipsec profile**  
**crypto isakmp key**  
**show isakmp key (IPsec)**

# tunnel remote id

**Overview** This command specifies a tunnel remote identifier sent to the peer for match.

Use the **no** variant of this command to remove the tunnel remote ID.

**Syntax** `tunnel remote id <1-2147483647>`  
`no tunnel remote id`

| Parameter      | Description                         |
|----------------|-------------------------------------|
| <1-2147483647> | Tunnel ID from 1 through 2147483647 |

**Default** No tunnel remote ID is set.

**Mode** Interface Configuration

**Usage notes** The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel remote ID on one endpoint must be specified as the tunnel local ID on the other endpoint.

The remote session ID defaults to the tunnel remote ID and the remote session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

**Examples** To specify a tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel remote id 22
```

To remove the tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel remote id
```

**Related commands** [tunnel local id](#)

**Validation Commands** [show interface tunnel \(L2TPv3\)](#)

# tunnel security-reprocessing

**Overview** Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

**Syntax** tunnel security-reprocessing  
no tunnel security-reprocessing

**Default** Security reprocessing is disabled by default.

**Mode** Global Configuration

**Usage notes** Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and\\_Configuration Guide](#).

**Example** To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

**Related commands** [show interface tunnel \(IPsec\)](#)

**Command changes** Version 5.4.8-0.2: command added

## tunnel source (L2TPv3)

**Overview** Use this command to specify a tunnel source for the tunnel interface. The tunnel source can be specified by using an interface name or an IPv4 address. The source address must be an existing IPv4 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

**Syntax** `tunnel source {<ipv4-addr>|<interface-name>}`  
`no tunnel source`

| Parameter                     | Description                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;ipv4-addr&gt;</i>      | <p>Specify the tunnel source IPv4 address for the tunnel interface in the dotted decimal format A.B.C.D.</p> <p>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.</p> |
| <i>&lt;interface-name&gt;</i> | <p>Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc).</p> <p>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.</p>                                |

**Mode** Interface Configuration

**Examples** To configure an L2TPv3 tunnel source IPv4 address, use the commands:

```
awplus# configure terminal
awplus# interface eth1
awplus(config-if)# ip address 1.1.1.1/24
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source 1.1.1.1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source eth2
```

To remove a tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

**Related commands** **interface tunnel (L2TPv3)**  
**tunnel destination (L2TPv3)**  
**tunnel mode l2tp v3**



# 52 Transitioning IPv4 to IPv6 Commands

- Contents**
- **Introduction** on page 2342
  - **4to6-mapping** on page 2343
  - **br-address (software)** on page 2344
  - **clear 4to6-mapping** on page 2345
  - **ip dns forwarding dns46** on page 2347
  - **ip dns forwarding dns64** on page 2350
  - **limits (4to6-mapping)** on page 2352
  - **map4to6 (4to6-mapping)** on page 2353
  - **map6to4 (4to6-mapping)** on page 2355
  - **mesh-mode** on page 2357
  - **method** on page 2358
  - **originator (4to6-mapping) (deprecated)** on page 2359
  - **responder (4to6-mapping) (deprecated)** on page 2360
  - **rule** on page 2361
  - **show 4to6-mapping** on page 2363
  - **show ip dns forwarding dns46** on page 2364
  - **show running-config software-configuration** on page 2365
  - **show software-configuration** on page 2366
  - **software-configuration** on page 2368
  - **tunnel destination (DS-Lite)** on page 2369
  - **tunnel mode ds-lite** on page 2370
  - **tunnel mode lw4o6** on page 2371
  - **tunnel mode map-e** on page 2372
  - **tunnel security-reprocessing** on page 2373
  - **tunnel software** on page 2374
  - **upstream-interface** on page 2375

# 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](#).

# 4to6-mapping

**Overview** Use this command to add an IPv4 to IPv6 address mapping set and enter the IPv4 to IPv6 Address Mapping Configuration mode.

Use the **no** variant of this command to remove an IPv4 to IPv6 address mapping set.

**Syntax** 4to6-mapping <name>  
no 4to6-mapping <name>

| Parameter | Description                   |
|-----------|-------------------------------|
| <name>    | The name of the 4to6 mapping. |

**Mode** Global Configuration

**Usage notes** In some computer networks, there are two separate networks that need to be connected together, but one network only has IPv4 and one only has IPv6. This mapping configuration allows you to specify mappings between the address ranges for use with transition technologies to connect those networks together.

**Example** To add an IPv4 to IPv6 address mapping set named 'test' and enter IPv4 to IPv6 Address Mapping Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)#
```

To remove an IPv4 to IPv6 address mapping set named 'test', use the commands:

```
awplus# configure terminal
awplus(config)# no 4to6-mapping test
```

**Related commands** [clear 4to6-mapping](#)  
[limits \(4to6-mapping\)](#)  
[map4to6 \(4to6-mapping\)](#)  
[show 4to6-mapping](#)

**Command changes** Version 5.5.0-2.0: command added

## 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                         |
|----------------|-------------------------------------|
| <ipv6-address> | 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

## clear 4to6-mapping

**Overview** Use this command to clear one, some, or all of the IPv4 to IPv6 address mappings that were automatically created by the DNS46 system.

This command runs in 3 modes:

- **all** - removes all entries installed by the specified system
- **exact** - removes an exact match
- **non-exact** - removes all entries that are contained by both the IPv4 and IPv6 subnets provided

**Syntax** `clear 4to6-mapping <name> responder all dns46`  
`clear 4to6-mapping <name> responder exact <ipv4-address> <ipv6-address>`  
`clear 4to6-mapping <name> responder [exact] <ipv4-subnet> <ipv6-prefix>`

| Parameter      | Description                                                       |
|----------------|-------------------------------------------------------------------|
| <name>         | The 4to6 mapping group name.                                      |
| all            | Remove all entries created by the specified system.               |
| exact          | Require an exact match on the IPv4 and IPv6 addresses or subnets. |
| <ipv4-address> | The IPv4 address uses the format A.B.C.D.                         |
| <ipv4-subnet>  | The IPv4 address uses the format A.B.C.D/M.                       |
| <ipv6-address> |                                                                   |
| <ipv6-prefix>  |                                                                   |

**Mode** Privileged Exec

**Example** To remove all entries installed by DNS46 in the 'test' 4 to 6 mapping, use the command:

```
awplus# clear 4to6-mapping test responder all dns46
```

To remove the mapping between 192.0.2.1 and 2001:db8::1, use the command:

```
awplus# clear 4to6-mapping test responder exact 192.0.2.1
2001:db8::1
```

To remove the mapping between 192.0.2.0/24 and 2001:db8::/120, use the command:

```
awplus# clear 4to6-mapping test responder exact 192.0.2.0/24
2001:db8::/120
```

To remove any mapping between 192.0.2.2 (with any IPv6 address), use the command:

```
awplus# clear 4to6-mapping test responder 192.0.2.2/32::/0
```

To remove any mapping between 2001:db8::2 (with any IPv4 address), use the command:

```
awplus# clear 4to6-mapping test responder 0.0.0.0
2001:db8::2/128
```

**Related commands** **4to6-mapping**  
**show 4to6-mapping**

**Command changes** Version 5.5.0-2.0: command added

## ip dns forwarding dns46

**Overview** Use this command to enable DNS46, which provides 4 to 6 mapping functionality within DNS relay. This feature allows for single IPv4 to IPv6 mappings to a mapping instance, such as NAT46.

Use the **no** variant of this command to disable DNS46 settings.

**Syntax** `ip dns forwarding dns46`  
`ip dns forwarding dns46 <name> [subnet [<ipv4-address/m>|<ipv6-address/prefix-length>]]`  
`no ip dns forwarding dns46`  
`no ip dns forwarding dns46 <name> [subnet [<ipv4-address/m>|<ipv6-address/prefix-length>]]`

| Parameter                    | Description                                                            |
|------------------------------|------------------------------------------------------------------------|
| <name>                       | The name of the 4to6 mapping instance.                                 |
| <ip-address/m>               | The IPv4 subnet to operate DNS46 over for the listed mapping instance. |
| <ipv6-address/prefix-length> | The IPv6 prefix to operate DNS46 over for the listed mapping instance. |

**Mode** Global Configuration

**Default** DNS46 is disabled by default. DNS46 does not have a default mapping instance. For a set mapping instance, it will operate on all subnets if none are configured.

**Usage notes** In some computer networks, there may be two separate networks that need to communicate with each other: one with only IPv4 and the other with only IPv6. DNS46 enables DNS A requests to flow from the IPv4 network to the IPv6 network and back. It provides the necessary mappings (from A to AAAA) to the mapping instance (NAT46).

**Examples** To enable DNS46, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46
```

To set the DNS46 mapping instance, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 nat46
```

To add a DNS46 mapping instance's IPv4 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 subnet 192.168.1.0/24
```

To add a DNS46 mapping instance's IPv6 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 subnet 2001:db8:1::/64
```

To disable DNS46, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46
```

To remove a DNS46 mapping instance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46
```

To remove a DNS46 mapping instance's IPv4 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
192.168.1.0/24
```

To remove a DNS46 mapping instance's IPv6 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
2001:db8:1::/64
```

To remove all a DNS46 mapping instance's subnets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
```



**Output** The following shows typical output.

**Example output from ip dns forwarding dns46**

If you are setting a DNS46 mapping instance but one is already set, the error and output is as follows:% DNS46 doesn't support multiple mapping instances

If you are adding a subnet to a dns46 mapping instance but the listed DNS46 mapping instance doesn't exist it will output:% DNS46 mapping instance '%s' doesn't exist.

**Related commands** [ip dns forwarding](#)  
[show 4to6-mapping](#)

**Command changes** Version 5.5.3-2.1: command added

## ip dns forwarding dns64

**Overview** Use this command to enable DNS64 translation, using the given map4to6 instance.

DNS64 implements DNS query translations between an IPv6 client subnet and IPv6 server subnet. Together with NAT64, this feature supports IPv6 clients in communicating with IPv4 servers by translating the addresses in DNS AAAA records.

When a DNS query is made for an IPv6 address (AAAA record), it will translate the AAAA record into an A record (which contains the IPv4 address).

Use the **no** variant of this command to disable DNS64 translating using the given map4to6 instance.

**Syntax** `ip dns forwarding dns64 <map4to6-instance>[translate-all]`  
`no ip dns forwarding dns64 <map4to6-instance>`

| Parameter                             | Description                                                                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;map4to6-instance&gt;</code> | The name of the 4to6 mapping instance.                                                                                                                                                                          |
| <code>translate-all</code>            | Apply DNS64 translation to all DNS AAAA requests, not just members of the configured 4to6-mapping instance map6to4 rule. This is useful for hosts that contact their local DNS server via link-local addresses. |

**Default** DNS64 is disabled by default and does not have a default mapping instance.

**Mode** Global Configuration

**Example** To enable DNS64 with a map4to6 instance, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ip dns forwarding dns46 nat64
```

To enable DNS64 with a map4to6 instance, and apply DNS64 translation to all DNS AAAA requests, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ip dns forwarding dns46 nat64 translate-all
```

To disable DNS64, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ip dns forwarding dns46 nat64
```

**Related commands** [ip dns forwarding](#)

**Command changes** Version 5.5.4-1.1: command added

# limits (4to6-mapping)

**Overview** Use this command to limit the dynamic 4to6 mappings created by DNS46. You can limit the maximum number and the maximum age of those dynamic mappings.

Use the **no** variant of this command to remove the configured size and age limits.

**Syntax** `limits dynamic {size <size-limit>|age <age-limit>}`  
`no limits dynamic {size|age}`

| Parameter    | Description                                                  |
|--------------|--------------------------------------------------------------|
| size         | Limit the maximum number of dynamic mappings.                |
| <size-limit> | The limit for the maximum number of dynamic mappings.        |
| age          | Limit the maximum age for mappings.                          |
| <age-limit>  | The limit for the age of unused dynamic mappings in seconds. |

**Default** There are no limits on the maximum number or maximum age of dynamic mappings.

**Mode** IPv4 to IPv6 Address Mapping Configuration

**Example** To limit the 4to6 mapping 'test' to a maximum of 500 dynamic mappings with a maximum age of 86400 seconds (24 hours), use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# limits dynamic size 500
awplus(config-4to6-mapping)# limits dynamic age 86400
```

To remove the limits on the 4to6 mapping 'test', use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no limits dynamic size
awplus(config-4to6-mapping)# no limits dynamic age
```

**Related commands** [4to6-mapping](#)  
[show 4to6-mapping](#)

**Command changes** Version 5.5.0-1.3: command added

# map4to6 (4to6-mapping)

**Overview** Use this command to specify the IPv4 to IPv6 address mapping.

Use the **no** variant of this command to remove the IPv4 to IPv6 address mapping.

**Syntax** `map4to6 single <ip-address> <ipv6-address> [ipv6-interface <interface>]`  
`map4to6 subnet <ip-address/m> <ipv6-address/prefix-length> [ipv6-interface <interface>]`  
`no map4to6 single <ip-address> <ipv6-address> [ipv6-interface <interface>]`  
`no map4to6 subnet <ip-address/m> <ipv6-address/prefix-length> [ipv6-interface <interface>]`

| Parameter                    | Description                                                                    |
|------------------------------|--------------------------------------------------------------------------------|
| single                       | Configure a single IPv4 to IPv6 mapping.                                       |
| <ip-address>                 | The IPv4 address to map.                                                       |
| <ipv6-address>               | The IPv6 address to map.                                                       |
| subnet                       | Map an entire subnet between IPv4 and IPv6.                                    |
| <ip-address/m>               | The IPv4 subnet to map.                                                        |
| <ipv6-address/prefix-length> | The IPv6 prefix to map.                                                        |
| ipv6-interface <interface>   | Specify the name of the interface to use to determine part of the IPv6 subnet. |

**Mode** IPv4 to IPv6 Address Mapping Configuration

**Usage notes** There are three supported mapping modes:

- **single** - maps a specific IPv4 address to a specific IPv6 address
- **subnet** - maps an IPv4 subnet into an IPv6 subnet
- **ipv6-interface** - use this mode if you have a dynamic IPv6 subnet assigned (by RA or DHCPv6) and want to use addresses from it.

The network component of the address on that interface will combine with the supplied IPv6 address/subnet and the IPv4 address to produce an IPv6 address. For example, if the interface is assigned 2001:db8:1::/64 and 192.168.1.1(in single mode), the resulting IPv6 address would be 2001:db8:1::192.168.1.1

**Example** To map all IPv4 addresses to the IPv6 subnet on eth1 (using zeros for the parts that are not specified by the subnet or IPv4 address), use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# map4to6 subnet 0.0.0.0/0 ::/96
ipv6-interface eth1
```

To remove that mapping, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no map4to6 subnet 0.0.0.0/0 ::/96
ipv6-interface eth1
```

**Related commands** **4to6-mapping**  
**map6to4 (4to6-mapping)**  
**show 4to6-mapping**

**Command changes** Version 5.5.3-2.1: command added

## map6to4 (4to6-mapping)

**Overview** Use this command to specify the IPv4 to IPv6 address mapping to use for the responding device (i.e. the destination of the first packet seen).

Use the **no** variant of this command to remove the IPv4 to IPv6 address mapping.

**Syntax** map6to4 single <ip-address> <ipv6-address>  
map6to4 subnet <ip-address/m> <ipv6-address/prefix-length>  
no map6to4 single <ip-address> <ipv6-address>  
no map6to4 subnet <ip-address/m> <ipv6-address/prefix-length>

| Parameter                    | Description                                 |
|------------------------------|---------------------------------------------|
| single                       | Configure a single IPv4 to IPv6 mapping.    |
| <ip-address>                 | The IPv4 address to map.                    |
| <ipv6-address>               | The IPv6 address to map.                    |
| subnet                       | Map an entire subnet between IPv4 and IPv6. |
| <ip-address/m>               | The IPv4 subnet to map.                     |
| <ipv6-address/prefix-length> | The IPv6 subnet to map.                     |

**Mode** IPv4 to IPv6 Address Mapping Configuration

**Usage notes** There are two supported mapping modes:

- **single** - maps a specific IPv4 address to a specific IPv6 address
- **subnet** - maps an IPv4 subnet into an IPv6 prefix. You could map all IPv4 addresses to 64::A.B.C.D by specifying 64::/96.

**Example** To map the IPv4 address 192.0.2.1 to IPv6 address 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# map6to4 single 192.0.2.1
2001:db8::1
```

To remove the mapping, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no map6to4 single 192.0.2.1
2001:db8::1
```

**Related commands** **4to6-mapping**  
**map4to6 (4to6-mapping)**  
**show 4to6-mapping**

**Command changes** Version 5.5.3-0.1: command added



## mesh-mode

**Overview** Use this command to enable mesh-mode. Mesh-mode enables software 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** Software 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 software named 'demo' to communicate with endpoints that share the same IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration demo
awplus(config-software)# mesh-mode
```

**Related commands** [show software-configuration](#)  
[software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

## method

**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                                     |
|-----------|-------------------------------------------------|
| static    | Software configuration is statically configured |
| dhcp      | 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](#)

**Command changes** Version 5.4.9-0.1: command added

# originator (4to6-mapping) (deprecated)

**Overview** This command has been deprecated in software version 5.5.4-1.1. Use the command **map4to6 (4to6-mapping)** instead.

# responder (4to6-mapping) (deprecated)

**Overview** This command has been deprecated in software version 5.5.4-1.1. Use the command **map6to4 (4to6-mapping)** instead.

# rule

**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                                                                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>rule &lt;0-65535&gt;</code>            | Rule ID is an integer in the range <1-65535>                                                                                                      |
| <code>ipv4-prefix &lt;ipv4-prefix&gt;</code> | IPv4 prefix (e.g. 192.0.2.0/24)                                                                                                                   |
| <code>ipv6-prefix &lt;ipv6-prefix&gt;</code> | IPv6 prefix (e.g. 2001:db8: :/32)                                                                                                                 |
| <code>ea-length &lt;0-48&gt;</code>          | Embedded address length is an integer in the range <0-48>.                                                                                        |
| <code>psid-length &lt;0-15&gt;</code>        | Port Set ID (PSID) length is an integer in the range <0-15>, the default length is 0.                                                             |
| <code>psid &lt;psid-value&gt;</code>         | Port Set ID (PSID) value is either decimal <0-65535> or hexadecimal with a leading 0x. Different PSID values guarantee non-overlapping port sets. |
| <code>offset &lt;0-16&gt;</code>             | Port Set ID (PSID) offset is an integer in the range <0-16>.                                                                                      |
| <code>forwarding</code>                      | 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 Softwire Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# softwire-configuration swconfig
awplus(config-softwire)# rule 1 ipv4-prefix 192.0.2.0/24 ipv6-
prefix 2001:db8:1::/48 ea-length 16 forwarding
awplus(config-softwire)# 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 Softwire Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# softwire-configuration swconfig
awplus(config-softwire)# no rule 1
```

**Related commands** [method](#)  
[show softwire-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# show 4to6-mapping

**Overview** Use this command to show all the IPv4 to IPv6 address mappings the system has. The output of this command includes manually configured mappings and the ones that the DNS46 component generated and installed.

**Syntax** show 4to6-mapping

**Mode** Privileged Exec

**Usage notes** Use the **no map4to6** or **no map6to4** commands to remove manually configured individual entries. Use the **clear 4to6-mapping** command to remove DNS46 entries.

**Example** To show IPv4 to IPv6 mapping instances, use the command:  
awplus# show 4to6-mapping

**Output** The following shows typical output.

## Example output from show 4to6-mapping

```
awplus#show 4to6-mapping
IPv4 to IPv6 Instances:

Mapping Instance: test
 Originator Mappings:
 user subnet mapping between 0.0.0.0/0 and ::/96 using ipv6
 subnet from eth1
 Responder Mappings:
 user single mapping between 192.0.2.1 and 2001:db8::1
```

**Related commands**

- [4to6-mapping](#)
- [clear 4to6-mapping](#)
- [map4to6 \(4to6-mapping\)](#)
- [map6to4 \(4to6-mapping\)](#)
- [ip dns forwarding dns46](#)
- [limits \(4to6-mapping\)](#)

**Command changes** Version 5.5.3-0.1: command added

# show ip dns forwarding dns46

**Overview** Use this command to view the DNS relay DNS46 settings. DNS46 is an IPv4 to IPv6 transitional technology, which is used in conjunction with NAT46.

**Syntax** show ip dns forwarding dns46

**Mode** User Exec

**Example** To view the DNS relay DNS46 settings, use the command:  
awplus# show ip dns forwarding dns46

**Output** The following shows typical output.

## Example output from show ip dns forwarding dns46

```
##This example shows DNS46 is enabled with an instance 'nat46' and some
IP subnets.

awplus#show ip dns forwarding dns46

Status : Enabled
Instance : nat46
IPv4 Ranges
 178.15.2.1/24
 10.0.0.0/8
 172.18.0.0/16
IPv6 Ranges
 f002::f1/16
 fff1::f1/16
```

**Related commands** [show ip dns forwarding](#)

**Command changes** Version 5.5.3-2.1: 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                                      |
|------------------------|--------------------------------------------------|
| <software-config-name> | 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** The following shows typical output.

## 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 fo
 rule 20 ipv4-prefix 192.168.2.0/24 ipv6-prefix 2001:db8:2000::/48 ea-length 16 fo
 rule 30 ipv4-prefix 192.168.3.0/24 ipv6-prefix 2001:db8:3000::/48 ea-length 16 fo
 !
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                                 |
|------------------------|---------------------------------------------|
| <software-config-name> | 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** The following shows typical output.

**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)
```

**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](#)  
[br-address \(software\)](#)  
[upstream-interface](#)  
[rule](#)

**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 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                                  |
|-------------------------------|----------------------------------------------|
| <i>&lt;interface-name&gt;</i> | 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 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 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, br1) |

**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

# 53 IPv6 Tunneling Commands

- Contents**
- **Introduction** on page 2377
  - **interface tunnel (IPv6)** on page 2378
  - **ip address (IP Addressing and Protocol)** on page 2379
  - **ip tcp adjust-mss** on page 2381
  - **ipv6 address** on page 2383
  - **ipv6 tcp adjust-mss** on page 2385
  - **mtu** on page 2387
  - **show interface tunnel (IPv6)** on page 2389
  - **tunnel destination (IPv6)** on page 2390
  - **tunnel dscp** on page 2392
  - **tunnel mode (IPv6)** on page 2393
  - **tunnel source (IPv6)** on page 2394
  - **tunnel ttl** on page 2396

# 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](#).

# 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.                                           |
| <code>secondary</code>                     | Secondary IP address.                                                                                            |
| <code>label</code>                         | Adds a user-defined description of the secondary IP address.                                                     |
| <code>&lt;label&gt;</code>                 | A user-defined description of the secondary IP address. Valid characters are any printable character and spaces. |

**Mode** Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

**Usage notes** To set the primary IP address on the interface, specify only **ip address** `<ip-addr/prefix-length>`. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

**NOTE:** Use `show ip address` instead of `show ip address secondary` when you need to view a secondary address configured on an interface. `show ip address` will only show the primary address, not a secondary address for an interface.

**Examples** To add the IP address 10.10.10.50/24 to the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the 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                                                            |
|------------|------------------------------------------------------------------------|
| <mss-size> | <64-1460> Specifies the MSS size in bytes.                             |
| pmtu       | 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

**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:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

**Usage notes** Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the **ipv6 enable** command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

**Examples** To assign the IPv6 address 2001:0db8::a2/64 to eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the tunnel tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface ppp0, use the 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**
- 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                                                            |
|------------|------------------------------------------------------------------------|
| <mss-size> | <64-1460> Specifies the MSS size in bytes.                             |
| pmtu       | 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.

**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 eth interface default is 1500 bytes.

**Syntax** mtu <68-1582>  
no mtu

| Parameter | Description                             |
|-----------|-----------------------------------------|
| <68-1582> | The Maximum Transmission size in bytes. |

**Default** The default MTU size, for example 1500 bytes for eth 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

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth0 with MTU 1200 and tunnel1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

**Examples** To configure an MTU size of 1555 bytes for tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1555
```

To restore the MTU size to the default MTU size of 1500 bytes on tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no mtu
```

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

**Command changes** Version 5.4.7-1.1: Behavior change when MTU set to less than 1500 on FS980M and GS980M.

Version 5.5.1-0.1: Layer 3 jumbo frames supported on SBx908 GEN2 and x950.

Version 5.5.1-1.2: Layer 3 jumbo frames supported on x530 and GS980MX.

Version 5.5.3-1.x Layer 3 jumbo frames supported on x240, SE240, x250, SE250, x540L, SE540L.

Version 5.5.5-0.1 Layer 3 jumbo frames supported on XS900MX, x550, x930, SBx81CFC960.



# 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 tunnel20, use the command:

```
awplus# show interface tunnel20
```

## Example output from the show interface tunnel command

```
awplus#show interface tunnel20
Interface tunnel20
 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:x.<br><br>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.<br><br>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                                                                                                                                                                                                                                                                                                       |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;ipv6-addr&gt;</i>      | <p>Specify the tunnel source IPv6 address for the IPv6 tunnel interface in the dotted decimal format x:x::x:x.</p> <p>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.</p> |
| <i>&lt;interface-name&gt;</i> | <p>Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc).</p> <p>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.</p>                                      |

**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 \(IPv6\)](#)