

AlliedWare Plus™ Release Note

Software Version 5.2.2

Upgrading from 5.2.1 to 5.2.2-0.3 for SwitchBlade x908, x900-12XT/S and x900-24 Series Switches

Acknowledgements.....	5
New features in AlliedWare Plus™ 5.2.2	6
RFCs and other standards supported by AlliedWare Plus™ 5.2.2	7
Command differences between 5.2.1-0.10 and 5.2.2-0.3 for SwitchBlade x908 and x900 series switches.....	9
List of removed commands.....	21
Details of new commands	22
802.1X commands.....	22
debug dot1x.....	22
dot1x control-direction	23
dot1x eap.....	24
dot1x eapol-version.....	25
dot1x keytransmit	26
dot1x max-reauth-req.....	27
show debugging dot1x.....	27
show dot1x diagnostics	28
show dot1x sessionstatistics.....	29
show dot1x statistics interface.....	30
show dot1x supplicant	31
show dot1x supplicant interface.....	33
AAA commands.....	35
aaa accounting auth-mac default	35
aaa accounting auth-web default.....	37
aaa accounting dot1x.....	39
aaa accounting login.....	41
aaa accounting update.....	43
aaa authentication auth-mac	44
aaa authentication auth-web.....	45
aaa authentication dot1x	46
aaa authentication login	47
aaa group server	49
accounting login.....	50
debug aaa.....	51
show debugging aaa.....	52
Authentication commands	53
auth critical	53
auth dynamic-vlan-creation.....	54
auth guest-vlan.....	55
auth host-mode.....	56
auth max-supplicant.....	57
auth reauthentication	58
auth supplicant-mac	59
auth timeout quiet-period.....	61

auth timeout reauth-period.....	62
auth timeout server-timeout.....	63
auth timeout supp-timeout.....	64
auth-mac enable.....	65
auth-mac method.....	66
auth-mac reauth-relearning.....	67
auth-web enable.....	68
auth-web forward.....	69
auth-web max-auth-fail.....	71
auth-web method.....	72
auth-web-server http-redirect.....	73
auth-web-server ipaddress.....	74
auth-web-server ping-poll enable.....	75
auth-web-server ping-poll failcount.....	76
auth-web-server ping-poll interval.....	77
auth-web-server ping-poll reauth-fresh.....	78
auth-web-server ping-poll timeout.....	79
auth-web-server port.....	80
auth-web-server redirect-url.....	81
auth-web-server session-keep.....	82
auth-web-server ssl.....	83
auth-web-server sslport.....	84
show auth-mac diagnostics.....	85
show auth-mac interface.....	86
show auth-mac sessionstatistics.....	88
show auth-mac statistics interface.....	88
show auth-mac supplicant.....	89
show auth-mac supplicant interface.....	89
show auth-web.....	90
show auth-web diagnostics.....	91
show auth-web interface.....	92
show auth-web sessionstatistics.....	93
show auth-web statistics interface.....	94
show auth-web supplicant.....	94
show auth-web supplicant interface.....	95
show auth-web-server.....	96
BGP commands.....	97
show bgp memory maxallocation.....	97
show debugging bgp.....	97
show ip bgp prefix-list.....	98
show ip bgp quote-regexp.....	98
show ip protocols bgp.....	99
Dynamic Host Configuration Protocol (DHCP) commands.....	100
ip dhcp-relay max-message-length.....	100
File management commands.....	101
copy current-software.....	101
copy debug.....	101
delete.....	102
delete debug.....	102
move debug.....	103
pwd.....	103
IGMP multicast commands.....	104
ip igmp ra-option (Router Alert).....	104
ip igmp robustness-variable.....	104
show debugging igmp.....	105

IP addressing and protocols commands	106
debug ip packet interface.....	106
ip irdp holdtime.....	107
Link aggregation commands	108
debug lacp	108
Local RADIUS server commands.....	109
attribute	109
authentication	111
group	112
crypto pki enroll local.....	113
crypto pki enroll local local-radius-all-users.....	114
crypto pki enroll local user.....	115
crypto pki export local pem.....	116
crypto pki export local pkcs12	117
crypto pki trustpoint local.....	118
debug crypto.....	119
nas	120
radius-server local	121
server auth-port.....	122
server enable.....	123
show crypto pki certificates.....	124
show crypto pki certificates local-radius-all-users	126
show crypto pki certificates user.....	127
show crypto pki trustpoints.....	128
show radius local-server group	129
show radius local-server nas	130
show radius local-server statistics	131
show radius local-server user	132
show radius local-server user	133
user (RADIUS server).....	134
vlan (RADIUS server)	135
OSPF commands	136
maximum-area	136
ospf restart grace-period.....	137
ospf restart helper.....	137
show ip protocols ospf	138
PIM Sparse Mode commands.....	139
ip pim anycast-rp	139
ip pim bsr-border.....	140
Quality of Service (QoS) commands.....	141
mls qos fabric-queue.....	141
mls qos map fabric-queue.....	143
mls qos map premark-dscp to.....	145
mls qos map policed-dscp to	146
set queue.....	147
show class-map.....	148
storm-protection	148
RADIUS commands.....	149
deadtime (Server Group).....	149
debug radius	150
ip radius source-interface.....	151
server (Server Group).....	152
show debugging radius	154
show radius.....	155
show radius statistics	157
RIP commands.....	158
rip restart grace-period	158

Secure Shell (SSH) commands	159
ssh server authentication.....	159
SNMP commands.....	160
snmp-server source-interface.....	160
Spanning tree commands.....	161
spanning-tree guard root	161
show debugging mstp	161
Stacking commands (SwitchBlade x908 only).....	162
stack software-auto-synchronization	162
Switching commands	163
clear mac address-table dynamic.....	163
clear mac address-table static.....	164
platform bist	165
platform control-plane-prioritization rate.....	165
platform load-balancing.....	167
platform routingratio	168
platform prbs	168
show mac address-table thrash-limit.....	169
thrash-limiting.....	169
System configuration and monitoring commands.....	171
debug nsm	171
debug nsm packet.....	171
max-fib-routes.....	171
max-static-routes	172
show system interrupts.....	173
show system pci device	174
show system pci tree	175
Trigger commands	176
trigger activate.....	176
VRRP commands	177
virtual-ip	177
vrrp vmac	177

Acknowledgements

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 licensed under the GNU General Public License available from:

<http://www.gnu.org/licenses/gpl2.html>

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Centre at:

<http://www.alliedtelesis.com/support/default.aspx>

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

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a cheque 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

Copyright © 2008 Allied Telesis, Inc. All Rights Reserved.

This documentation is subject to change without notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of Allied Telesis, Inc.

Allied Telesis and AlliedWare Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Caution: Using a software maintenance version for the wrong model may cause unpredictable results, including disruption to the network.

Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New features in AlliedWare Plus™ 5.2.2

High Speed Stacking

With AlliedWare Plus™ 5.2.2, the SwitchBlade x908 Advanced Layer 3+ Modular Switch uses dedicated ports on the rear of its chassis to perform highspeed stacking. This feature is available only on the SwitchBlade x908 switch.

Control Plane Prioritization

The Control Plane Prioritization (CPP) feature allows you to allocate priorities to packet types, to ensure minimum interruption to the flow of control information through the network. This feature is available on x900 and SwitchBlade x908 switches.

See the [platform control-plane-prioritization rate](#) command for more information about this.

Network Access Control

AlliedWare Plus 5.2.2 supports NAC by using 802.1X port-based authentication with standards compliant dynamic VLAN assignment. This feature enables a user's adherence to the network's security policies to be assessed and authentication either granted or remediation offered. NAC supports alternatives to 802.1X port based authentication, such as web authentication to enable guest access, and MAC authentication for end points that do not have an 802.1x supplicant.

See the [802.1X commands](#), [AAA commands](#), [Authentication commands](#), and [Local RADIUS server commands](#) sections of this document for a detailed list of the new commands.

Dynamic VLAN Assignment

Dynamic VLAN assignment allows an 802.1X supplicant to be placed into a specific VLAN based on information returned from the RADIUS server during authentication. This limits the network access of a supplicant to a specific VLAN that is tied to their authentication, and prevents supplicants from connecting to VLANs for which they are not authorized. A port's VLAN assignment is determined by the first supplicant to be authenticated on the port.

See the [vlan \(RADIUS server\)](#) command for information about dynamic vlan using RADIUS.

Loop Protection

Loop Protection - Thrash Limiting, detects and resolves network loops. It is highly user-configurable - from the rate of looping traffic to the type of action the switch should take when it detects a loop.

See the [thrash-limiting](#) command for information about this feature.

STP Root Guard

STP Root Guard designates which devices can assume the role of Root Bridge in an STP network. This stops an undesirable device from taking over this role, where it could either compromise network performance or cause a security weakness.

See the [spanning-tree guard root](#) command for information about the STP Root Guard.

Dynamic Link Failover

Dynamic Link Failover (Host Attach) is a versatile feature that enables devices that do not support link aggregation to form multiple active links, by using triggers and scripts. You can customize Dynamic Link Failover to suit almost any situation, from a simple redundant backup link to multiple active links capable of basic load-sharing.

See the Triggers Introduction, Triggers Configuration, and Trigger Command chapters of the AlliedWare Plus™ OS Software Reference for software version 5.2.2 for more information.

Advanced Storm Control

Packet storm protection allows you to set limits on the reception rate of broadcast, multicast frames and destination lookup failures. You can set separate limits for each of the different packet types. Policy-based storm protection allows you to define the traffic rate that creates a broadcast storm. You can also configure the action the switch takes when it detects a storm. See the [storm-protection](#) command for more information.

Standards and protocols: SwitchBlade x908 and x900 series switches

Standards and Protocols

AlliedWare Plus™ Operating System Version 5.2.2

Authentication

- RFC 1321 MD5 Message-Digest Algorithm
- RFC 1828 IP Authentication using Keyed MD5

Border Gateway Protocol (BGP)

- BGP Dynamic Capability
- BGP Graceful Restart
- BGP Outbound Route Filtering
- Extended Communities Attribute
- RFC 1771 Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of the Border Gateway Protocol in the Internet
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2439 BGP Route Flap Damping
- RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP
- RFC 2858 Multiprotocol Extensions for BGP-4
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4

Encryption

- FIPS 180-1 Secure Hash Standard (SHA-1)
- FIPS 186 Digital Signature Standard (RSA)
- FIPS 46-3 Data Encryption Standard (DES & 3DES)

Ethernet

- IEEE 802.2 Logical Link Control
- IEEE 802.3 Ethernet CSMA/CD
- IEEE 802.3ab 100BASE-T
- IEEE 802.3ad Link Aggregation
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae 10 Gigabit Ethernet
- IEEE 802.3u 100BASE-T
- IEEE 802.3x Flow Control - Full Duplex Operation
- IEEE 802.3z Gigabit Ethernet

General Routing

- ECMP Equal Cost Multi Path routing
- RFC 768 User Datagram Protocol (UDP)
- RFC 791 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 Transmission Control Protocol (TCP)
- RFC 826 Address Resolution Protocol (ARP)
- RFC 894 Standard for the transmission of IP datagrams over Ethernet networks
- RFC 903 Reverse ARP
- RFC 919 Broadcasting Internet Datagrams
- RFC 922 Broadcasting Internet Datagrams in the presence of subnets
- RFC 925 Multi-LAN ARP
- RFC 932 Subnetwork addressing scheme
- RFC 950 Internet Standard Subnetting Procedure
- RFC 951 Bootstrap Protocol (BootP) relay and server
- RFC 1027 Proxy ARP
- RFC 1035 DNS Client

- RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
- RFC 1071 Computing the Internet checksum
- RFC 1122 Internet Host Requirements
- RFC 1191 Path MTU discovery
- RFC 1256 ICMP Router Discovery Messages
- RFC 1518 An Architecture for IP Address Allocation with CIDR
- RFC 1519 Classless Inter-Domain Routing (CIDR)
- RFC 1542 Clarifications & Extensions for the Bootstrap Protocol
- RFC 1700 Assigned Numbers
- RFC 1812 Requirements for IPv4 Routers
- RFC 1918 IP Addressing
- RFC 2131 DHCP for IPv4
- RFC 2132 DHCP Options and BOOTP Vendor Extensions.
- RFC 2581 TCP Congestion Control
- RFC 3046 DHCP Relay Agent Information Option (DHCP Option 82)
- RFC 3232 Assigned Numbers
- RFC 3993 Subscriber-ID Suboption for DHCP Relay Agent Option

IPv6 Features

- RFC 1886 DNS Extensions to support IPv6
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2460 IPv6 specification
- RFC 2461 Neighbour Discovery for IPv6
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 ICMPv6
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526 Reserved IPv6 Subnet Anycast Addresses
- RFC 2711 IPv6 Router Alert Option
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3484 Default Address Selection for IPv6
- RFC 3513 IPv6 Addressing Architecture
- RFC 3587 IPv6 Global Unicast Address Format

Management

- AT Enterprise MIB
- Control Plane Prioritisation
- Loop Protection
- RFC 1155 Structure and Identification of Management Information for TCP/IP-based Internets
- RFC 1157 Simple Network Management Protocol (SNMP)
- RFC 1212 Concise MIB definitions
- RFC 1213 MIB for Network Management of TCP/IP-based internets: MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1227 SNMP MUX protocol and MIB
- RFC 1239 Standard MIB
- RFC 1493 Bridge MIB
- RFC 2011 SNMPv2 MIB for IP using SMIv2
- RFC 2012 SNMPv2 MIB for TCP using SMIv2
- RFC 2013 SNMPv2 MIB for UDP using SMIv2
- RFC 2096 IP Forwarding Table MIB

- RFC 2239 IEEE 802.3 MAU MIB
- RFC 2574 User-based Security Model (USM) for SNMPv3
- RFC 2575 View-based Access Control Model (VACM) for SNMP
- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions (VLAN)
- RFC 2741 Agent Extensibility (AgentX) Protocol
- RFC 2790 Host MIB
- RFC 2819 RMON MIB
- RFC 2863 Interfaces Group MIB
- RFC 3164 Syslog Protocol
- RFC 3412 Message Processing and Dispatching for the SNMP
- RFC 3413 SNMP Applications
- RFC 3418 MIB for SNMP
- RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types
- RFC 4188 Definitions of Managed Objects for Bridges
- RFC 4318 Definitions of Managed Objects for Bridges with RSTP

SNMP Traps Triggers

Multicast Support

- Bootstrap Router for PIM-SM
- IGMP & MLD snooping switches
- IGMP Proxy
- IGMP Snooping
- RFC 1112 Host extensions for IP multicasting
- RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
- RFC 2362 PIM-SM
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 3376 IGMPv3

Open Shortest Path First (OSPF)

- Graceful OSPF Restart
- OSPF Link-local Signaling
- OSPF MD5 Authentication
- OSPF Restart Signaling
- OSPF TE Extensions
- Out-of-band LSDB Resync
- RFC 1245 OSPF protocol analysis
- RFC 1246 Experience with the OSPF protocol
- RFC 1370 Applicability Statement for OSPF
- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPFv2
- RFC 2370 OSPF Opaque LSA Option
- RFC 3101 OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3509 Alternative Implementations of OSPF Area Border Routers

Quality of Service

- ACLs Access Control Lists
- DiffServ
- IEEE 802.1p Priority Tagging
- RFC 2211 Specification of the Controlled-Load Network Element Service

Standards and protocols: SwitchBlade x908 and x900 series switches

RFC 2474	Definition of the Differentiated Services Field (DS Field)
RFC 2475	An Architecture for Differentiated Services
RFC 2597	Assured Forwarding PHB Group
RFC 2697	A Single-Rate Three-Color Marker
RFC 2698	A Two-Rate Three-Color Marker
RFC 3246	Expedited Forwarding PHB (Per-Hop Behavior)

Resiliency Features

Dynamic Link Failover	
EPSR Ethernet Protection Switched Rings	
IEEE 802.1D Spanning Tree Protocol (STP) - MAC Bridges	
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)	
IEEE 802.1t 802.1D maintenance	
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)	
RFC 3768	Virtual Router Redundancy Protocol (VRRP)
STP Root Guard	

Routing Protocols

RFC 1058	Routing Information Protocol (RIP)
RFC 2080	RIPng for IPv6
RFC 2082	RIP-2 MD5 Authentication
RFC 2453	RIPv2
Route Maps	
Route Redistribution	

Security Features

BPDU Protection	
Dynamic VLAN Assignment	
Guest VLAN support (IEEE 802.1x)	
IEEE 802.1x Port Based Network Access Control	
IEEE 802.1x Authentication protocols (TLS, TTLS, PEAP & MD5)	
IEEE 802.1x Multi Supplicant authentication	
MAC-based authentication	
Port Security	
RFC 2246	TLS Protocol v1.0
RFC 2865	RADIUS
RFC 2866	RADIUS Accounting
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 3546	Transport Layer Security (TLS) Extensions
RFC 3748	PPP Extensible Authentication Protocol (EAP)
RFC 4251	Secure Shell (SSHv2) Protocol Architecture
RFC 4252	Secure Shell (SSHv2) Authentication Protocol
RFC 4253	Secure Shell (SSHv2) Transport Layer Protocol
RFC 4254	Secure Shell (SSHv2) Connection Protocol
SSH Remote Login	
SSLv2	
SSLv3	
Web-based Authentication	

Services

Ping Polling	
RFC 854	Telnet protocol specification
RFC 855	Telnet Option Specifications
RFC 857	Telnet Echo Option
RFC 858	Telnet Suppress Go Ahead Option
RFC 1091	Telnet terminal-type option
RFC 1305	NTPv3
RFC 1350	Trivial File Transfer Protocol (TFTP)
RFC 1985	SMTP Service Extension
RFC 2049	MIME
RFC 2554	SMTP Service Extension for Authentication
RFC 2616	Hypertext Transfer Protocol - HTTP/1.1
RFC 2821	Simple Mail Transfer Protocol (SMTP)
RFC 2822	Internet Message Format
SCP	Secure Copy

VLAN Support

IEEE 802.1ad	VLAN double tagging (Q-in-Q)
IEEE 802.1Q	Virtual LANs
IEEE 802.1v	VLAN classification by protocol & port
IEEE 802.3ac	VLAN tagging
Private VLANs	

Command differences between 5.2.1-0.10 and 5.2.2-0.3 for SwitchBlade x908 and x900 series switches

For new and changed commands, please note that equivalent changes have been made to the related **no** commands. These are not included in the table below.

For changed commands, differences are highlighted in **bold**.

Details of most of the new commands can be found later in this release note.

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
AAA, authentication, 802.1x, RADIUS commands	aaa accounting auth-mac (default) (start-stop stop-only none) {group (radius GROUP-NAME)}	–
	aaa accounting auth-web (default) (start-stop stop-only none) {group (radius GROUP-NAME)}	–
	aaa accounting dot1x (default) (start-stop stop-only none) {group (radius GROUP-NAME)}	–
	aaa accounting login (default LIST-NAME) (start-stop stop-only none) {group (radius GROUP-NAME)}	–
	aaa accounting update (periodic <1-65535>)	–
	aaa authentication auth-mac (default) {group (radius GROUP-NAME)}	–
	aaa authentication auth-web (default) {group (radius GROUP-NAME)}	–
	aaa authentication dot1x (default) {group (radius GROUP-NAME)}	–
	aaa authentication login (default LIST-NAME) {local group (radius GROUP-NAME)}	–
	aaa group server (radius) GROUP-NAME	–
	aaa local authentication attempts lockout-time <0-10000>	–
	aaa local authentication attempts max-fail <1-32>	–
	clear aaa local user lockout {username WORD all}	–
	accounting login (default LIST-NAME)	–

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
AAA, authentication, 802.1x, RADIUS commands continued	attribute (NAME) help	–
	attribute NAME VALUE	–
	auth critical	–
	auth dynamic-vlan-creation (rule (deny permit))	–
	auth guest-vlan <1-4094>	–
	auth host-mode (single-host multi-host multi-supplicant)	–
	auth max-supplicant <2-1024>	–
	auth supplicant-mac MAC	–
	auth supplicant-mac MAC{port-control (auto force-authorized force-unauthorized) quiet-period <1-65535> reauth-period <1-4294967295> supp-timeout <1-65535> server-timeout <1-65535> reauthentication max-reauth-req <1-10>}	–
	auth reauthentication	–
	auth timeout quiet-period <1-65535>	–
	auth timeout reauth-period <1-4294967295>	–
	auth timeout server-timeout <1-65535>	–
	auth timeout supp-timeout <1-65535>	–
	–	auth-mac auth-fail-action (restrict-vlan <2-4094> drop-traffic)
	–	auth-mac dynamic-vlan-creation (enable disable)
	–	auth-mac mac-aging (enable disable)
	auth-mac method (eap-md5 pap)	–
	auth-mac reauth-relearning	–
	auth-web enable	–
	auth-web forward (arp dhcp dns tcp <1-65535> udp <1-65535>)	–
	auth-web max-auth-fail <0-10>	–
	auth-web method (eap-md5 pap)	–
	auth-web-server enable	–
auth-web-server http-redirect	–	

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
AAA, authentication, 802.1x, RADIUS commands continued	auth-web-server ipaddress A.B.C.D	–
	auth-web-server ping-poll enable	–
	auth-web-server ping-poll failcount <1-100>	–
	auth-web-server ping-poll interval <1-65535>	–
	auth-web-server ping-poll reauth-timer-refresh	–
	auth-web-server ping-poll timeout <1-30>	–
	auth-web-server port PORTNO	–
	auth-web-server redirect-url URL	–
	auth-web-server refresh	–
	auth-web-server session-keep	–
	auth-web-server ssl	–
	auth-web-server sslport PORTNO	–
	authentication (mac eapmd5 eaptls peap)	–
	cd (flash nvs card debug WORD)	cd (flash nvs card WORD)
	clear radius-server (dot1x auth-mac auth-web) type {authentication accounting}	–
	copy local-radius-user-db (flash nvs card debug tftp scp WORD)	–
	copy WORD local-radius-user-db (add replace)	–
	copy WORD web-auth-https-file	–
	debug aaa (authentication accounting all)	–
	debug dot1x auth-web	–
	debug radius (packet event all)	–
	–	dot1x dynamic-vlan-creation (enable disable)
	dot1x control-direction (in both)	–
	dot1x eap (discard forward forward-untagged-vlan forward-vlan)	–
	dot1x eapol -version <1-2>	dot1x protocol-version <1-2>
	dot1x max-reauth-req <1-10>	dot1x max-req <1-10>

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
AAA, authentication, 802.1x, RADIUS commands continued	dot l x reauthenticate interface IFNAME	dot l x re-authenticate interface IFNAME
	dot l x system-auth-ctrl	–
	erase web-auth-https-file	–
	ip radius source-interface (IFNAME A.B.C.D)	–
	login authentication (default LIST-NAME)	–
	radius local-server import user-db WORD (add replace)	–
	radius-server accounting (dot l x auth-mac auth-web) enable	–
	radius-server accounting (dot l x auth-mac auth-web) stop-only	–
	radius-server accounting interval <1-65535>	–
	radius-server accounting update	–
	radius-server deadtime <0-1440>	radius-server deadtime MIN
	radius-server host (dot l x auth-mac auth-web) HOSTNAME	radius-server host HOSTNAME
	radius-server host (dot l x auth-mac auth-web) HOSTNAME {key STRING retransmit RETRIES timeout SEC auth-port PORTNO acct-port PORTNO deadtime MIN }	radius-server host HOSTNAME {key STRING retransmit RETRIES timeout SEC auth-port PORTNO}
	radius-server host (HOSTNAME A.B.C.D) ({auth-port <0-65535> acct-port <0-65535>}){timeout <1-1000> retransmit <0-100> key STRING})	–
	radius-server key STRING	radius-server key KEY
	radius-server local	–
	radius-server retransmit <0-100>	radius-server retransmit RETRIES
	radius-server timeout <1-1000>	radius-server timeout SEC
	show auth-web-server	–
	show debugging aaa	–
show debugging radius	–	
show radius	–	
show radius local-server error	–	
show radius local-server group (WORD)	–	

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
AAA, authentication, 802.1x, RADIUS commands continued	show radius local-server nas (A.B.C.D))	–
	show radius local-server statistics	–
	show radius local-server user	–
	show radius local-server user format csv	–
	show radius local-server user format user-name-only	–
	show radius local-server user WORD	–
	show radius local-server user WORD format csv	–
	show radius statistics	–
	undebg dot1x auth-web	–
	undebg radius (packet event all)	–
	user WORD password WORD (group WORD)	–
ACL, IP community list and QoS commands	access-list <3000-3699> (deny permit send-to-cpu copy-to-cpu copy-to-mirror) <other-parameters> ({vlan <1-4094> inner-vlan <1-4094>})	access-list <3000-3699> (deny permit send-to-cpu copy-to-cpu copy-to-mirror) <other-parameters>
	ip community-list <1-99> (deny permit) [AA:NN local-AS no-advertise no-export]	ip community-list <1-99> (deny permit) LINE
	ip community-list standard WORD (deny permit) [AA:NN local-AS no-advertise no-export]	ip community-list standard WORD (deny permit) LINE
	ip community-list WORD (deny permit) [AA:NN local-AS no-advertise no-export]	ip community-list WORD (deny permit) LINE
	match dscp <0-63>	–
	mls qos aggregate-police NAME (single-rate) <1-16000000> <0-16777216> <0-16777216> action (drop-red policed-dscp-transmit)	mls qos aggregate-police NAME (single-rate) <1-16000000> <0-16777216> <0-16777216> exceed-action (drop policed-dscp-transmit)
	mls qos aggregate-police NAME (twin-rate) <1-16000000> <1-16000000> <0-16777216> <0-16777216> action (drop-red policed-dscp-transmit)	mls qos aggregate-police NAME (twin-rate) <1-16000000> <1-16000000> <0-16777216> <0-16777216> exceed-action (drop policed-dscp-transmit)
mls qos fabric -queue <0-3> (<0-3> (<0-3> (<0-3>))) (priority wrr (weight <1-30>))	mls qos input-queue <0-3> (<0-3> (<0-3> (<0-3>))) (priority wrr (weight <1-30>))	

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
File management commands	copy (flash nvs card debug http tftp scp sftp) (flash nvs card debug tftp scp) WORD	copy (flash nvs card http tftp scp sftp) (flash nvs card tftp scp) WORD
	copy (flash nvs card debug http tftp scp sftp WORD) (flash nvs card debug tftp scp WORD)	copy (flash nvs card http tftp scp sftp WORD) (flash nvs card tftp scp WORD)
	copy running-config (flash nvs card debug tftp scp WORD)	copy running-config (flash nvs card tftp scp WORD)
	copy startup-config (flash nvs card debug tftp scp WORD)	copy startup-config (flash nvs card tftp scp WORD)
	delete ({force recursive }) (flash nvs card debug WORD)	delete ({force recursive }) (flash nvs card WORD)
	dir (all) (recursive) (flash nvs card debug WORD)	dir (all) (recursive) (flash nvs card WORD)
	move (flash nvs card debug WORD) (flash nvs card debug WORD)	move (flash nvs card WORD) (flash nvs card WORD)
PKI commands	crypto pki enroll local	–
	crypto pki enroll local local-radius-all-users	–
	crypto pki enroll local user WORD	–
	crypto pki export local pem url WORD	–
	crypto pki export local pkcs12 WORD WORD	–
	crypto pki trustpoint local	–
	debug crypto pki	–
	show crypto pki certificates (local-ca local)	–
	show crypto pki certificates local-radius-all-users	–
	show crypto pki certificates user (WORD)	–
	show crypto pki trustpoints	–
SNMP and RMON commands	debug snmp all	–
	debug snmp detail	–
	debug snmp error-string	–
	debug snmp process	–
	debug snmp receive	–

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
SNMP and RMON commands continued	debug snmp send	–
	debug snmp xdump	–
	rmon alarm <I-65535> (WORD) interval <I-4294967295> (delta absolute) rising-threshold <0-2147483647> event <I-65535> falling-threshold <0-2147483647> event <I-65535> (owner WORD)	rmon alarm <I-65535> (WORD) interval <I-65535> (delta absolute) rising-threshold <0-2147483647> event <I-65535> falling-threshold <0-2147483647> event <I-65535> (owner WORD)
	rmon clear counters	–
	rmon debug	–
	show running-config rmon	–
	snmp-server source-interface (traps informs) IFNAME	–
	trap	–
	undebug snmp all	–
	undebug snmp detail	–
	undebug snmp error-string	–
	undebug snmp process	–
	undebug snmp receive	–
	undebug snmp send	–
undebug snmp xdump	–	
IP and DHCP commands	ip dhcp-relay max-message-length <548-1472>	–
	ip gratuitous-arp-link <0-300>	–
	lease <0-30> <0-24> <0-60> (<0-60>)	lease <0-30> <0-24> <0-60>
	neighbor (A.B.C.D X:X::X:X WORD) advertisement-interval <0-600>	neighbor (A.B.C.D X:X::X:X WORD) advertisement-interval <I-600>
	show ip rip database (full)	show ip rip database
	undebug ip packet (interface WORD)	–

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
IGMP and PIM commands	ip igmp robustness-variable <1-7>	ip igmp robustness-variable <2-7>
	ip igmp static-group A.B.C.D{(source (A.B.C.D ssm-map))}(interface IFRANGE)}	ip igmp static-group A.B.C.D{(source (A.B.C.D ssm-map))}(interface IFNAME)}
	ip pim anycast-rp A.B.C.D A.B.C.D	–
	ip pim bsr-border	–
	ip pim rp-address A.B.C.D (<1-99> <1300-1999> WORD) (override)	ip pim rp-address A.B.C.D (<1-99> <1300-1999> WORD)
	ip pim rp-candidate IFNAME (priority <0-255>) (group-list (<1-99> WORD)) (interval <1-16383>)	ip pim rp-candidate IFNAME (priority <0-255>) (group-list (<1-99> <1300-1999> WORD)) (interval <1-16383>)
	ip pim unicast-bsm	–
	show ip igmp snooping statistics interface IFRANGE group (A.B.C.D)	show ip igmp snooping statistics interface IFNAME
BGP commands	show ip bgp (unicast multicast)	show ip bgp ipv4 (unicast multicast)
	show ip bgp (unicast multicast) A.B.C.D	show ip bgp ipv4 (unicast multicast) A.B.C.D
	show ip bgp (unicast multicast) A.B.C.D/M	show ip bgp ipv4 (unicast multicast) A.B.C.D/M
	show ip bgp (unicast multicast) A.B.C.D/M longer-prefixes	show ip bgp ipv4 (unicast multicast) A.B.C.D/M longer-prefixes
	show ip bgp (unicast multicast) cidr-only	show ip bgp ipv4 (unicast multicast) cidr-only
	show ip bgp (unicast multicast) community	show ip bgp ipv4 (unicast multicast) community
	show ip bgp (unicast multicast) community [AA:NN local-AS no-advertise no-export] (exact-match)	show ip bgp ipv4 (unicast multicast) community [AA:NN local-AS no-advertise no-export] (exact-match)
	show ip bgp (unicast multicast) community-list WORD (exact-match)	show ip bgp ipv4 (unicast multicast) community-list WORD (exact-match)
	show ip bgp (unicast multicast) dampening dampened-paths	show ip bgp ipv4 (unicast multicast) dampening dampened-paths
	show ip bgp (unicast multicast) dampening flap-statistics	show ip bgp ipv4 (unicast multicast) dampening flap-statistics
	show ip bgp (unicast multicast) dampening parameters	show ip bgp ipv4 (unicast multicast) dampening parameters
	show ip bgp (unicast multicast) filter-list WORD	show ip bgp ipv4 (unicast multicast) filter-list WORD
	show ip bgp (unicast multicast) inconsistent-as	show ip bgp ipv4 (unicast multicast) inconsistent-as
	show ip bgp (unicast multicast) neighbors	show ip bgp ipv4 (unicast multicast) neighbors
	show ip bgp (unicast multicast) neighbors (A.B.C.D X::X:X)	show ip bgp ipv4 (unicast multicast) neighbors (A.B.C.D X::X:X)

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
BGP commands continued	show ip bgp (unicast multicast) neighbors (A.B.C.D X::X:X) advertised-routes	show ip bgp ipv4 (unicast multicast) neighbors (A.B.C.D X::X:X) advertised-routes
	show ip bgp (unicast multicast) neighbors (A.B.C.D X::X:X) received prefix-filter	show ip bgp ipv4 (unicast multicast) neighbors (A.B.C.D X::X:X) received prefix-filter
	show ip bgp (unicast multicast) neighbors (A.B.C.D X::X:X) received-routes	show ip bgp ipv4 (unicast multicast) neighbors (A.B.C.D X::X:X) received-routes
	show ip bgp (unicast multicast) neighbors (A.B.C.D X::X:X) routes	show ip bgp ipv4 (unicast multicast) neighbors (A.B.C.D X::X:X) routes
	show ip bgp (unicast multicast) paths	show ip bgp ipv4 (unicast multicast) paths
	show ip bgp (unicast multicast) prefix-list WORD	show ip bgp ipv4 (unicast multicast) prefix-list WORD
	show ip bgp (unicast multicast) quote-regexp WORD	show ip bgp ipv4 (unicast multicast) quote-regexp WORD
	show ip bgp (unicast multicast) regexp LINE	show ip bgp ipv4 (unicast multicast) regexp LINE
	show ip bgp (unicast multicast) route-map WORD	show ip bgp ipv4 (unicast multicast) route-map WORD
	show ip bgp (unicast multicast) summary	show ip bgp ipv4 (unicast multicast) summary
	show ip bgp view WORD (unicast multicast) summary	show ip bgp view WORD ipv4 (unicast multicast) summary
		show bgp quote-regexp WORD
		show bgp regexp LINE
VRRP and virtual commands	router vrrp <I-255> IFNAME	-
	show vrrp <I-255> IFNAME	show vrrp <I-255>
	show virtual-servers	-
	virtual-ip A.B.C.D owner	-
	virtual-server (tcp udp) <0-65535> A.B.C.D <0-65535> WORD	-

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
Server commands	server (HOSTNAME A.B.C.D) ({auth-port <0-65535> acct-port <0-65535>})	–
	server auth-port <1-65535>	–
	server enable	–
Spanning tree commands	spanning-tree enable	–
	spanning-tree hello-time <1-10>	–
	spanning-tree mst instance <1-15> restricted-role	–
	spanning-tree mst instance <1-15> restricted-tcn	–
	spanning-tree restricted-role	–
	spanning-tree restricted-tcn	–
	spanning-tree shutdown	–
	spanning-tree transmit-holdcount <1-10>	–
Stacking commands	show stack full-debug (<1-8>)	show stack full-debug
	stack <1-8> software-auto-synchronize	–
	stack all software-auto-synchronize	–
Other commands	deadtime <0-1440>	–
	cvlan registration table WORD (bridge <1-32>)	–
	flowcontrol both	–
	fullupdate	–
	group WORD	–
	mac address-table thrash-limit (<5-255>)	–
	show mac address-table thrash-limit	–
	thrash-limiting {action (learn-disable link-down port-disable vlan-disable none) timeout (<0-86400>)}	–

Feature	5.2.2-0.3 commands	5.2.1-0.10 commands
Other commands continued	nas A.B.C.D key WORD	–
	debug platform packet ({ recv send vlan (<1-4094> all) timeout <0-3600> })	debug platform packet ((recv send) ((timeout <0-3600>)))
	show debugging platform packet	–
	debug nsm ha (all)	–
	undebug nsm ha	–
	undebug nsm ha all	–
	vlan WORD	–
	wait <1-65535>	–
no maximum-prefix	no maximum-prefix <1-65535> <1-100>	

List of removed commands

The following commands were available in 5.2.1 and have been removed. Please note that configuration scripts that use these commands will either automatically update to the new commands, or will still function.

802.1X commands dot1x protocol-version <1-2>
no dot1x protocol-version

Access Control List commands maximum-access-list <1-4294967294>
no maximum-access-list

Authentication commands auth-mac auth-fail-action (restrict-vlan <2-4094>|drop-traffic)

QoS commands no mls qos map mark-dscp (<0-63>|)
no match ip-dscp
show mls qos maps mark-dscp (<0-63>|)

Stacking commands stack <1-8> autoupgrade

Switching commands show thrash-limiting (IFNAME)

User Authentication commands clear pam local user lockout (username WORD | all)
no pam local authentication attempts lockout-time
no pam local authentication attempts max-fail
pam local authentication attempts lockout-time <0-10000>
pam local authentication attempts max-fail <1-32>

VRRP commands no interface

Details of new commands

802.1X commands

debug dot1x

Use this command to enable 802.1X IEEE Port-Based Network Access Control troubleshooting functions. Use the **no** parameter with this command to disable this function.

Syntax `debug dot1x [all|auth-web|event|nsm|packet|timer]`
`no debug all dot1x`
`no debug dot1x [all|auth-web|event|nsm|packet|timer]`

Parameter	Description
all	Used with the no form exclusively; turns off all debugging for 802.1X
auth-web	Specifies debugging for 802.1X auth-web information
events	Specifies debugging for 802.1X events
nsm	Specifies debugging for NSM messages
packet	Specifies debugging for 802.1X packets
timer	Specifies debugging for 802.1X timers

Mode Privileged Exec mode and Global Configuration mode

Usage This command without any parameters turns on normal 802.1X debug information.

```
awplus#debug dot1x
awplus#show debugging dot1x
```

```
802.1X debugging status:
 802.1X events debugging is
 802.1X timer debugging is on
 802.1X packets debugging is on
 802.1X NSM debugging is on
```

Examples

```
awplus#debug dot1x
awplus#debug dot1x all
```

Related Commands [show debugging dot1x](#)

dot1x control-direction

This command sets the direction of the filter for the unauthorized port.

If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the packets received from the supplicant.

If the optional **both** parameter is specified with this command then packets entering and leaving the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.

The **no dot1x control-direction** command sets the direction of the filter to **both**. The port discards egress traffic.

Syntax dot1x control-direction {in|both}
no dot1x control-direction

Parameter	Description
no	Negate a command or set its defaults
dot1x	IEEE 802.1X Port-Based Access Control
control-direction	Specify packet control direction
in	Discard received packets from the supplicant
both	Discard received packets from the supplicant and transmitted packets to the supplicant

Default The authentication port direction is set to **both** by default.

Mode Interface mode

Example To set the port direction to the default (**both**) for port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no dot1x control-direction
```

To set the port direction to **in** for port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#dot1x control-direction in
```

Validation Commands show dot1x
show dot1x interface
show auth-mac interface
show auth-web interface

dot1x eap

This command selects the transmit mode for the EAP packet. If the authentication feature is not enabled then EAP transmit mode is not enabled. The default setting discards EAP packets.

Syntax `dot1x eap {discard|forward|forward-untagged-vlan|forward-vlan}`

Parameter	Description
<code>dot1x</code>	IEEE 802.1X Port-Based Access Control
<code>eap</code>	EAP packets
<code>discard</code>	Discard
<code>forward</code>	Forward to all ports on the switch
<code>forward-untagged-vlan</code>	Forward to ports with the same untagged vlan
<code>forward-vlan</code>	Forward to ports with the same vlan

Default The transmit mode is set to `discard` EAP packets by default.

Mode Global Configuration mode

Example To set the transmit mode of EAP packet to `forward` to forward EAP packets to all ports on the switch, use the following commands:

```
awplus#configure terminal
awplus(config)#dot1x eap forward
```

To set the transmit mode of EAP packet to `discard` to discard EAP packets, use the following commands:

```
awplus#configure terminal
awplus(config)#dot1x eap discard
```

To set the transmit mode of EAP packet to `forward-untagged-vlan` to forward EAP packets to ports with the same untagged vlan, use the following commands:

```
awplus#configure terminal
awplus(config)#dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to `forward-vlan` to forward EAP packets to ports with the same vlan, use the following commands:

```
awplus#configure terminal
awplus(config)#dot1x eap forward-vlan
```

dot1x eapol-version

This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the **no dot1x eapol-version** command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

Syntax dot1x eapol-version <1-2>

no dot1x eapol-version

Parameter	Description
no	Negate a command or set its defaults
dot1x	IEEE 802.1X Port-Based Access Control
eapol-version	Set the protocol version
<1-2>	EAPOL version (default 1)

Default The EAP version for 802.1X authentication is set to 1 by default.

Mode Interface mode

Example To set the EAPOL protocol version to 2 for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no dot1x eapol-version
```

Validation Commands show dot1x
show dot1x interface

dot1x keytransmit

This command enables key transmission on the interface specified previously in Interface mode. The **no dot1x keytransmit** command disables key transmission on the interface specified.

Syntax dot1x keytransmit
no dot1x keytransmit

Parameter	Description
no	Negate a command or set its defaults
dot1x	IEEE 802.1X Port-Based Access Control
keytransmit	Transmit 802.1X authentication key

Default Key transmission for port authentication is enabled by default.

Usage Use this command to enable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant. Use the **no** version of this command to disable key transmission.

Mode Interface mode

Example To enable the key transmit feature on interface port 1.0.2, after it has been disabled by negation, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#dot1x keytransmit
```

To disable the key transmit feature from the default startup configuration on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no dot1x keytransmit
```

Validation Commands show dot1x
show dot1x interface

dot1x max-reauth-req

This command sets the number of reauthentication attempts before an interface is unauthorized.

The **no dot1x max-reauth-req** command resets the reauthentication delay to the default (2).

Syntax dot1x max-reauth-req <1-10>

no dot1x max-reauth-req

Parameter	Description
no	Negate a command or set its defaults
dot1x	IEEE 802.1X Port-Based Access Control
max-reauth-req	Number of reauthentication attempts before becoming unauthorized (default 2)
<1-10>	Count

Default The default maximum reauthentication count for port authentication is 2.

Usage Use this command to set the maximum reauthentication attempts after failure.

Mode Interface mode

show debugging dot1x

Use this command to display the 802.1X debugging option set.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token.

Syntax show debugging dot1x

Mode Privileged Exec mode

Usage This is a sample output from the show debugging dot1x command.

```
awplus#debug dot1x
awplus#show debugging dot1x
```

```
802.1X debugging status:
 802.1X events debugging is on
 802.1X timer debugging is on
 802.1X packets debugging is on
 802.1X NSM debugging is on
```

Example

```
awplus#show debugging dot1x
```

Related Commands debug dot1x

show dot1x diagnostics

This command shows 802.1X authentication diagnostics for the specified interface (optional).

If no interface is specified then authentication diagnostics are shown for all interfaces.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token.

Syntax `show dot1x diagnostics [interface <ifrang>]`

Parameter	Description
show	Show running system information
dot1x	IEEE 802.1X Port-Based Access Control
diagnostics	Diagnostics
interface	Specify an interface to show
<ifrang>	Interface range

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing 802.1X authentication diagnostics for port 1.0.12:

```
awplus#show dot1x diagnostics interface port1.0.12
```

```
Authentication Diagnostics for interface port1.0.12
  Supplicant address: 00d0.59ab.7037
  authEnterConnecting: 2
  authEaplogoffWhileConnecting: 1
  authEnterAuthenticating: 2
  authSuccessWhileAuthenticating: 1
  authTimeoutWhileAuthenticating: 1
  authFailWhileAuthenticating: 0
  authEapstartWhileAuthenticating: 0
  authEaplogoggWhileAuthenticating: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
  BackendResponses: 2
  BackendAccessChallenges: 1
  BackendOtherrequestToSupplicant: 3
  BackendAuthSuccess: 1
```

show dot1x sessionstatistics

This command shows authentication session statistics for the specified interface.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token.

Syntax `show dot1x sessionstatistics [interface <ifrang>]`

Parameter	Description
show	Show running system information
dot1x	IEEE 802.1X Port-Based Access Control
sessionstatistics	Session statistics
interface	Specify an interface to show
<ifrang>	Interface range

Mode Exec mode and Privileged Exec mode

Example See sample output below showing 802.1X authentication session statistics for port 1.0.12:

```
awplus#show dot1x sessionstatistics interface port1.0.12
```

```
Authentication session statistics for interface port1.0.12
session user name: manager
session authentication method: Remote server
session time: 19440 secs
session terminat cause: Not terminated yet
```

show dot1x statistics interface

This command shows the authentication statistics for the specified interface.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token.

Syntax `show dot1x statistics interface <ifranger>`

Parameter	Description
show	Show running system information
dot1x	IEEE 802.1X Port-Based Access Control
statistics	Statistics
interface	Specify an interface to show
<ifranger>	Interface range

Mode Exec mode and Privileged Exec mode

Example See sample output below showing 802.1X authentication statistics for port 1.0.12:

```
awplus#show dot1x statistics interface port1.0.12
```

```
802.1X statistics for interface port1.0.12
EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

show dot1x supplicant

This command shows the supplicant state of the authentication mode set for the switch.

This command shows a summary when the optional **brief** parameter is used.

Syntax show dot1x supplicant [*<macadd>*] [brief]

Parameter	Description
show	Show running system information
dot1x	IEEE 802.1X Port-Based Access Control
supplicant	Specify a supplicant to show
<i><macadd></i>	Mac (hardware) address of the Supplicant
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus#show dot1x supplicant
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
authenticationMethod: dot1x
portStatus: Authorized - currentId: 4
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the brief parameter:

```
awplus#show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.12
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Interface VID Mode MAC Address Status IP Address Username
===== ==  ==  =====  =====  =====  =====
port1.0.12 2 D 00d0.59ab.7037Authenticated 192.168.2.201 manager
```

Related Commands [show dot1x supplicant interface](#)

show dot1x supplicant interface

This command shows the supplicant state of the authentication mode set for the interface.

This command shows a summary when the optional **brief** parameter is used.

Syntax `show dot1x supplicant interface <ifrangle> [brief]`

Parameter	Description
show	Show running system information
dot1x	IEEE 802.1X Port-Based Access Control
supplicant	Specify a supplicant to show
interface	Specify an interface to show
<ifrangle>	Interface range
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example See sample output below showing the supplicant on the interface port 1.0.12:

```
awplus#show dot1x supplicant interface port1.0.12
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
authenticationMethod: dot1x
portStatus: Authorized - currentId: 4
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the brief parameter:

```
awplus#show dot1x supplicant interface brief
```

```
Interface port1.0.12
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Interface VID Mode MAC Address Status IP Address Username
===== == == == ===== =====
port1.0.12 2 D 00d0.59ab.7037Authenticated 192.168.2.201 manager
```

Related Commands [show dot1x supplicant](#)

AAA commands

aaa accounting auth-mac default

This command configures a default accounting server for MAC-based Authentication. The default accounting option specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting option is automatically applied to interfaces with MAC-based Authentication enabled.

There are two options 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

Configure the **group-name** using the **aaa group server** command. Configure the RADIUS server for **group radius** using the **radius-server host** command.

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Use the **no aaa accounting auth-mac** command to disable AAA accounting for MAC-based Authentication globally.

Syntax `aaa accounting auth-mac default {start-stop|stop-only|none}
group {<group-name>|radius}`

`no aaa accounting auth-mac default`

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
accounting	Configure accounting parameters
auth-mac	Set accounting server for auth-mac
default	Default accounting server
start-stop	Start and stop records to be sent
stop-only	Stop records to be sent
none	No accounting record to be sent
group	Use a server group
radius	Use all RADIUS servers
<group-name>	Server group name

Default RADIUS accounting for MAC-based Authentication is disabled by default

Mode Global Configuration mode

Example To enable RADIUS accounting for MAC-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus#configure terminal
awplus(config)#aaa accounting auth-mac default start-stop group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus#configure terminal
awplus(config)#no aaa accounting auth-mac default
```

Related Commands [aaa authentication auth-mac](#)

aaa accounting auth-web default

This command configures a default accounting server for Web-based Port Authentication. The default accounting option specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting option is automatically applied to interfaces with Web-based Authentication enabled.

There are two options 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

Configure the **group-name** using the **aaa group server** command. Configure the RADIUS server for **group radius** using the **radius-server host** command.

Configure the accounting event to be sent to the RADIUS server with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Use the **no aaa accounting auth-web** command to disable AAA accounting for Web-based Port Authentication globally.

Syntax

```
aaa accounting auth-web default {start-stop|stop-only|none}
    group {<group-name>|radius}

no aaa accounting auth-web default
```

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
accounting	Configure accounting parameters
auth-web	Set accounting server for auth-web
default	Default accounting server
start-stop	Start and stop records to be sent
stop-only	Stop records to be sent
none	No accounting record to be sent
group	Use a server group
radius	Use all RADIUS servers
<group-name>	Server group name

Default RADIUS accounting for WEB-based Port Authentication is disabled by default.

Mode Global Configuration mode

Example To enable RADIUS accounting for Web-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus#configure terminal
awplus(config)#aaa accounting auth-web default start-stop group radius
```

To disable RADIUS accounting for Web-based Authentication, use the commands:

```
awplus#configure terminal
awplus(config)#no aaa accounting auth-web default
```

Related Commands [aaa authentication auth-web](#)

aaa accounting dot1x

This command configures the default accounting server for IEEE 802.1x-based Authentication. The default accounting option specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting option is automatically applied to interfaces with IEEE 802.1x-based Authentication enabled.

There are two options 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

Configure the **group-name** using the **aaa group server** command. Configure the RADIUS server for **group radius** using the **radius-server host** command.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Use the **no aaa accounting dot1x** command to disable AAA accounting for 802.1x-based Port Authentication globally.

Syntax

```
aaa accounting dot1x default {start-stop|stop-only|none}
    group {<group-name>|radius}

no aaa accounting dot1x default
```

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
accounting	Configure accounting parameters
dot1x	Set accounting server for 802.1X
default	Default accounting server
start-stop	Start and stop records to be sent
stop-only	Stop records to be sent
none	No accounting record to be sent
group	Use a server group
radius	Use all RADIUS servers
<group-name>	Server group name

Default RADIUS accounting for 802.1X-based Port Authentication is disabled by default. (There is no default server set by default).

Mode Global Configuration mode

Usage Use this command to enable accounting on all switch ports with 802.1X enabled, and to specify which accounting messages to send and the ordered list of servers to use for accounting. Use the **no** version of this command to remove the default accounting server for 802.1X. This disables 802.1X accounting.

Example To enable RADIUS accounting for 802.1x-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus#configure terminal
awplus(config)#aaa accounting dot1x default start-stop group radius
```

To disable RADIUS accounting for 802.1x-based Authentication, use the commands:

```
awplus#configure terminal
awplus(config)#no aaa accounting dot1x default
```

Related Commands

- aaa accounting update
- aaa authentication dot1x
- aaa group server
- dot1x port-control
- radius-server host

aaa accounting login

This command configures RADIUS accounting for a login shell session. The specified server name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, the default (Accounting for login sessions is disabled) is applied to every console and vty line unless another accounting server is applied on that line.

Use the **no aaa accounting login** command to remove an accounting server for a login shell session configured by an **aaa accounting login** command. If the server being deleted is already applied to a console or vty line, accounting on that line will be disabled. If the default server 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|<group-name>}}
```

```
no aaa accounting login {default|<list-name>}
```

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
accounting	Configure accounting parameters
login	Set authentication server for login session
default	Default accounting server
<list-name>	Named accounting server
start-stop	Start and stop records to be sent
stop-only	Stop records to be sent
none	No accounting record to be sent
group	Use server group
radius	Use all RADIUS servers
<group-name>	Server group name

Usage This command enables you to define a named accounting server. 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 server (the the name `default`) and any number of other named servers. The `<list-name>` for any server that you define can then be used as the `<list-name>` parameter in the **accounting login** command available from Line Configuration mode.

If the server name already exists, the command will replace the existing configuration with the new one. There are two options 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

Configure the **group-name** using the **aaa group server** command. Configure the RADIUS server for **group radius** using the **radius-server host** command.

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Default RADIUS accounting is disabled by default for all login shell sessions.

Mode Global Configuration mode

Example To configure RADIUS accounting for login shell session, use the following commands:

```
awplus#configure terminal
awplus(config)#aaa accounting login default start-stop group radius
```

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 authentication login](#)
[aaa accounting login](#)
[accounting login](#)

aaa accounting update

This command enables periodic accounting reporting to the RADIUS accounting server(s) wherever RADIUS accounting has been configured.

When periodic accounting report is enabled, interim accounting records are sent periodically according to the specified interval in the **periodic** parameter. The default interval is 30 minutes.

Use the **no aaa accounting update** command to disable periodic accounting reporting to the RADIUS accounting server(s).

Syntax `aaa accounting update [periodic <1-65535>]`
`no aaa accounting update`

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
accounting	Configure accounting parameters
update	Configure interim accounting update
periodic	Send accounting records periodically
<1-65535>	Intervals to send accounting update (in minutes)

Default Periodic accounting update is disabled by default.

Mode Global Configuration mode

Usage Use this command to enable the device to send periodic AAA accounting reports to the accounting server. When periodic accounting updates are enabled, interim accounting records are sent periodically at the specified intervals. Use the **no** version of this command to disable periodic accounting updates to the accounting server.

Example To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus#configure terminal
awplus(config)#aaa accounting update periodic 10
```

To disable periodic accounting update wherever RADIUS accounting has been configured, use the following commands:

```
awplus#configure terminal
awplus(config)#no aaa accounting update
```

Related Commands [aaa accounting auth-mac default](#)
[aaa accounting auth-web default](#)
[aaa accounting dot1x](#)

aaa authentication auth-mac

This command enables MAC-based Port Authentication globally and allows you to specify an authentication server. It is automatically applied to every interface running MAC-based Port Authentication.

There are two options to define servers where RADIUS authentication 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

Configure the **group-name** using the `aaa group server` command. Configure the RADIUS server for **group radius** using the `radius-server host` command.

Use the `no aaa authentication auth-mac` command to globally disable MAC-based Port Authentication.

Syntax `aaa authentication auth-mac default group {<group-name>|radius}`
`no aaa authentication auth-mac default`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>aaa</code>	Authentication, Authorization and Accounting
<code>authentication</code>	Configure Authentication parameters
<code>auth-mac</code>	Set authentication server for auth-mac
<code>default</code>	Default authentication server
<code>group</code>	Use server group
<code>radius</code>	Use all RADIUS servers
<code><group-name></code>	Server group name

Default MAC-based Port Authentication is disabled by default.

Mode Global Configuration mode

Example To enable MAC-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus#configure terminal
awplus(config)#aaa authentication auth-mac default group radius
```

To disable MAC-based Port Authentication, use the commands:

```
awplus#configure terminal
awplus(config)#no aaa authentication auth-mac default
```

Related Commands `aaa accounting auth-mac default`
`auth-mac enable`

aaa authentication auth-web

This command enables Web-based Port Authentication globally and allows you to enable an authentication server. It is automatically applied to every interface running Web-based Port Authentication.

There are two options to define servers where RADIUS authentication 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

Configure the **group-name** using the `aaa group server` command. Configure the RADIUS server for **group radius** using the `radius-server host` command.

Use the `no aaa authentication auth-web` command to globally disable Web-based Port Authentication.

Syntax `aaa authentication auth-web default group {<group-name>|radius}`
`no aaa authentication auth-web default`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>aaa</code>	Authentication, Authorization and Accounting
<code>authentication</code>	Configure Authentication parameters
<code>auth-web</code>	Set the authentication server for auth-web
<code>default</code>	Default authentication server list
<code>group</code>	Use server group
<code>radius</code>	Use all RADIUS servers
<code><group-name></code>	Server group name

Default Web-based Port Authentication is disabled by default.

Mode Global Configuration mode

Example To enable Web-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus#configure terminal
awplus(config)#aaa authentication auth-web default group radius
```

To disable Web-based Port Authentication, use the commands:

```
awplus#configure terminal
awplus(config)#no aaa authentication auth-web default
```

Related Commands `aaa accounting auth-web default`
`auth-mac enable`

aaa authentication dot1x

This command enables 802.1X-based Port Authentication globally and allows you to enable an authentication server. It is automatically applied to every interface running 802.1X-based Port Authentication.

There are two options to define servers where RADIUS authentication 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

Configure the **group-name** using the **aaa group server** command. Configure the RADIUS server for **group radius** using the **radius-server host** command.

Use the **no aaa authentication dot1x** command to globally disable 802.1X-based Port Authentication.

Syntax `aaa authentication dot1x default group {<group-name> | radius}`
`no aaa authentication dot1x default`

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
authentication	Configure Authentication parameters
dot1x	Set authentication server for auth-mac
default	Default authentication server
group	Use server group
radius	Use all RADIUS servers
<group-name>	Server group name

Default 802.1X-based Port Authentication is disabled by default.

Mode Global Configuration mode

Usage Use this command to specify the default server to use for authentication on all switch ports with 802.1X enabled. Use the **no** version of this command to reset the default authentication server for 802.1X, to its default, that is, to use the group **radius**, containing all RADIUS servers configured by the **radius-server host** command.

Example To enable 802.1X-based Port Authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:

```
awplus#configure terminal
awplus(config)#aaa authentication dot1x default group radius
```

To disable 802.1X-based Port Authentication, use the command:

```
awplus#configure terminal
awplus(config)#no aaa authentication dot1x default
```

Related Commands

- aaa accounting dot1x
- aaa group server
- dot1x port-control
- radius-server host

aaa authentication login

Use this command to create an ordered list of servers to use to authenticate user login, or to replace an existing server with the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** server name is specified, it is applied to every console and VTY line immediately unless another server is applied to that line by the **login authentication** command. To apply a non-default server, you must also use the **login authentication** command.

Use the **no** version of this command to remove an authentication server for user login. The specified server name is deleted from the configuration. If the server 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 server. This will return the default server to its default state (**local** is the default).

Syntax

```
aaa authentication login {default|<list-name>} [local]
    [group {radius|<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 radius	Use all RADIUS servers configured by the radius-server host command.
group <group-name>	Use the specified RADIUS server group, as configured by the aaa group server command.

Default If the default server is not configured using this command, user login authentication uses the local user database only. If the **default** server name is specified, it is applied to every console and VTY line immediately unless another server is applied to that line by the **login authentication** command.

local is the default state for the default server. Reset to the default server using the **no aaa authentication login default** command.

Mode Global Configuration mode

Examples To configure the default authentication server for user login to use all available RADIUS servers and then the local user database, use the following commands:

```
awplus#configure terminal
awplus(config)#aaa authentication login default group radius local
```

To configure a user login authentication server called `USERS` to use first the local user database and then the RADIUS server group `RAD_GROUP1` for user login authentication, use the following commands:

```
awplus#configure terminal
awplus(config)#aaa authentication login USERS local group RAD_GROUP1
```

To return to the default server (**local** is the default server), use the following commands:

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

To delete an existing authentication server `USERS` created for user login authentication, use the following commands:

```
awplus#configure terminal
awplus(config)#no aaa authentication login USERS
```

Related Commands [login authentication](#)

aaa group server

This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in **aaa** commands. The group name **radius** is predefined, which includes all RADIUS servers configured by the **radius-server host** command.

RADIUS servers are added to a server group using the **server** command. Each RADIUS server should be configured using the **radius-server host** command. Use the **no aaa group** command to remove an existing RADIUS server group.

Syntax `aaa group server radius <group-name>`

`no aaa group server`

Parameter	Description
no	Negate a command or set its defaults
aaa	Authentication, Authorization and Accounting
group	Configure AAA group
server	Configure AAA server group
radius	Configure RADIUS server group
<group-name>	Server-group name

Mode Global Configuration mode

Usage Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the **radius-server host** command. To add RADIUS servers to a server group, use the **server** command.

Example 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
```

accounting login

This command applies a login accounting server to console or vty lines for user login. When login accounting is enabled using the **aaa accounting login** command, logging events generate an accounting record to the accounting server configured using **aaa accounting login**.

The accounting server must be configured first using the **aaa accounting login** command. If an accounting server is specified that has not been created by the **aaa accounting login** command then accounting will be disabled on the specified lines.

The **no accounting login** command resets AAA (Authentication, Authorization, Accounting) Accounting applied to console or vty lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

Syntax `accounting login [default|<list-name>]`
`no accounting login`

Parameter	Description
no	Negate a command or set its defaults
accounting	Configure accounting parameters
login	Set accounting server for login session
default	Default accounting server
<list-name>	Named accounting server

Default By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using the **aaa accounting login** command beforehand.

Mode Line mode

Example 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 login](#)

debug aaa

This command enables AAA debugging.

- If **authentication** is specified with **debug aaa**, debugging for AAA authentication is enabled.
- If **accounting** is specified with **debug aaa**, debugging for AAA accounting is enabled.
- If **all** is specified with **debug aaa**, all debugging options are enabled.
- If no option is specified with **debug aaa**, all debugging options are enabled.

Use the **no debug aaa** command to disable AAA debugging.

- If **authentication** is specified with **no debug aaa**, debugging for AAA authentication is disabled.
- If **accounting** is specified with **no debug aaa**, debugging for AAA accounting is disabled.
- If **all** is specified with **no debug aaa**, all debugging options are disabled.
- If no option is specified with **no debug aaa**, all debugging options are disabled.

Syntax `debug aaa [accounting|all|authentication]`
`no debug aaa [accounting|all|authentication]`

Parameter	Description
no	Negate a command or set its defaults
debug	Debugging functions (see also 'undebug')
aaa	Authentication, Authorization and Accounting
authentication	Authentication
accounting	Accounting
all	Turn on all debugging

Default AAA debugging is disabled by default.

Mode Privileged Exec mode

Example 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](#)

show debugging aaa

This command displays the current debugging status for AAA (Authentication, Authorization, Accounting).

Syntax show debugging aaa

Parameter	Description
show	Show running system information
debugging	Debugging functions (see also 'undebug')
aaa	Authentication, Authorization and Accounting

Mode Privileged Exec mode

Example To display the current debugging status of AAA, use the command:

```
awplus#show debug aaa
```

```
AAA debugging status:  
Authentication debugging is on  
Accounting debugging is off
```

Authentication commands

auth critical

This command enables the critical port feature on the interface specified. When the critical port feature is enabled on a port and all the RADIUS servers are unavailable, then the port becomes authorized.

The **no auth critical** command disables critical port feature on the interface.

Syntax `auth critical`
`no auth critical`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
critical	Operation in case there is no response from radius server

Default The critical port of port authentication is disabled.

Mode Interface mode

Example To enable the critical port feature on interface port 1.0.2, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth critical
```

To disable the critical port feature on interface port 1.0.2, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth critical
```

Validation Commands `show auth-web-server`
`show dot1x`
`show dot1x interface`

auth dynamic-vlan-creation

The Dynamic VLAN assignment feature allows a supplicant to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given port. This command enables and disables the Dynamic VLAN assignment feature. Use the **no auth dynamic-vlan-creation** command to disable the Dynamic VLAN assignment feature.

If the Dynamic VLAN assignment feature is enabled (disabled by default), VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports.

The **rule** parameter specifies the VLAN assignment rule when the second supplicant's VLAN ID is different from VLAN ID from the first supplicant. If the **deny** value is applied with the command then the second supplicant with a different VLAN ID is rejected. If the **permit** value is applied with the command then the second supplicant with a different VLAN ID is accepted and assigned to the first supplicant's VLAN.

Syntax `auth dynamic-vlan-creation [rule {deny|permit}]`

`no auth dynamic-vlan-creation`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
dynamic-vlan-creation	Dynamic vlan creation
rule	VLAN assignment rule
deny	Deny a differently assigned VLAN ID
permit	Permit a differently assigned VLAN ID

Default The dynamic vlan of port authentication is disabled.

Mode Interface mode

Example To enable the Dynamic VLAN assignment feature on interface port 1.0.2, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth dynamic-vlan-creation
```

To disable the Dynamic VLAN assignment feature on interface port 1.0.2, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth dynamic-vlan-creation
```

Validation Commands `show dot1x`
`show dot1x interface`

Related Commands `auth host-mode`

auth guest-vlan

This command enables the guest vlan feature on the switch port specified by associating a guest VLAN with a switch port. This command does not start authentication. The supplicant's traffic is associated with the native VLAN of the port if its not already associated with another VLAN.

The **no auth guest-vlan** command disables the guest vlan feature on the interface specified.

Syntax `auth guest-vlan <1-4094>`

`no auth guest-vlan`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
guest-vlan	set guest vlan
<1-4094>	VLAN ID (VID)

Default The guest vlan authentication feature is disabled by default.

Mode Interface mode

Usage The guest VLAN may be used by supplicants (client devices) that have not attempted authentication, or have failed the authentication process. Note that if a port is in multi-supplicant mode with per-port dynamic VLAN configuration, after the first successful authentication, subsequent hosts cannot use the guest VLAN due to the change in VLAN ID. This may be avoided by using per-user dynamic VLAN assignment.

When using the guest VLAN feature with the multi-host mode, a number of supplicants can communicate via a guest VLAN before authentication. A supplicant's traffic is associated with the native VLAN of the specified switch port. The supplicant must belong to a VLAN before traffic from the supplicant can be associated.

Example To set the guest vlan feature to vlan 100 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth guest-vlan 100
```

To disable the guest vlan feature on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth guest-vlan
```

Validation Commands `show dot1x`
`show dot1x interface`

auth host-mode

This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X. Use the **no auth host-mode** command to set host mode to the default setting (single host).

Syntax `auth host-mode {single-host|multi-host|multi-supPLICANT}`
`no auth host-mode`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
host-mode	Set host-mode on a port
single-host	Single host mode
multi-host	Multi host mode
multi-supPLICANT	Multi supplicant mode

Default The default host mode for port authentication is for a single host.

Mode Interface mode

Example To set the host mode to multi-supPLICANT on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth host-mode multi-supPLICANT
```

To set the host mode to default (single host) on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth host-mode
```

Validation Commands `show dot1x`
`show dot1x interface`

auth max-supPLICant

This command sets the maximum number of supplicants on the interface that can be authenticated. After this value is exceeded supplicants are not authenticated.

The **no auth max-supPLICant** command resets the maximum supplicant number to the default (1024).

Syntax `auth max-supPLICant <2-1024>`
`no auth max-supPLICant`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
max-supPLICant	Max supplicant for port
<2-1024>	Limit number

Default The max supplicant of port authentication is 1024.

Mode Interface mode

Example To set the maximum number of supplicants to 10 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth max-supPLICant 10
```

To reset the maximum number of supplicant to default on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth max-supPLICant
```

Validation Commands `show dot1x`
`show dot1x interface`

auth reauthentication

This command enables re-authentication on the interface specified in the Interface mode.

Use the **no auth reauthentication** command to disables reauthentication on the interface.

Syntax `auth reauthentication`
`no auth reauthentication`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
reauthentication	Enable reauthentication on a port

Default Reauthentication of port authentication is disabled by default.

Mode Interface mode

Example To enable reauthentication on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awpluls(config)#interface port1.0.2
awplus(config-if)#auth reauthentication
```

To disable reauthentication on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awpluls(config)#interface port1.0.2
awplus(config-if)#no auth reauthentication
```

Validation Commands `show dot1x`
`show dot1x interface`

auth supplicant-mac

This command adds a supplicant mac address on a given port with the parameters as specified in the table below.

Use the **no auth supplicant-mac** command to delete the supplicant MAC address added by the **auth supplicant-mac** command, and resets to the default for the supplicant parameter.

Syntax

```
auth supplicant <mac-addr>
    [max-reauth-req <1-10>]
    [port-control {auto | force-authorized | force-unauthorized}]
    [quiet-period <1-65535>]
    [reauth-period <1-4294967295>]
    [supp-timeout <1-65535>]
    [server-timeout <1-65535>][reauthentication]
```

```
no auth supplicant-mac <macadd> [reauthentication]
```

Parameter	Description
no	Negate a command or set its defaults
auth	IEEE 802.1X Port-Based Access Control (Port Authentication)
supplicant-mac	Enable port authentication specified MAC address
<mac-addr>	MAC (hardware) address of the Supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format
port-control	Port control commands
auto	Allow port client to negotiate authentication
force-authorized	Force port state to authorized
force-unauthorized	Force port state to unauthorized
quiet-period	Quiet period in the HELD state (default 60 seconds)
<1-65535>	Seconds for quiet period
reauth-period	Seconds between reauthorization attempts (default 3600 seconds)
<1-4294967295>	Seconds for reauthorization attempts (reauth-period)
supp-timeout	Supplicant response timeout (default 30 seconds)
<1-65535>	Seconds for supplicant response timeout
server-timeout	Authentication server response timeout (default 30 seconds)
<1-65535>	Seconds for authentication server response timeout
reauthentication	Enable reauthentication on a port
max-reauth-req	No of reauthentication attempts before becoming unauthorized (default 2)
<1-10>	Count of reauthentication attempts

Default No supplicant MAC address for port authentication exists by default until first created with the **auth supplicant-mac** command. The defaults for parameters applied are as shown in the table.

Mode Interface mode

Example To add the supplicant MAC address 00:09:41:A4:59:43 for force authorized port control for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth supplicant-mac 0009.41A4.5943 port-control
force-authorized
```

To delete the supplicant MAC address 00:09:41:A4:59:43 for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth supplicant-mac 0009.41A4.5943
```

To reset reauthentication to disable for the supplicant MAC address 00:09:41:A4:59:43, for interface port 1.0.2 use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth supplicant-mac 0009.41A4.5943
reauthentication
```

Validation show dot1x
Commands show dot1x interface

auth timeout quiet-period

This command sets the time period for which the authentication request is not accepted on a given port, after the authentication request has failed an authentication.

Use the **no auth timeout quiet-period** command to reset quiet period to the default (60 seconds).

Syntax `auth timeout quiet-period <1-65535>`

`no auth timeout quiet-period`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
timeout	Set a timeout parameter
quiet-period	Quiet period in the HELD state (default is 60 seconds)
<1-65535>	Seconds

Default The quiet period of port authentication is 60 seconds.

Mode Interface mode

Example To set the quiet period to 10 for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth timeout quiet-period
```

auth timeout reauth-period

This command sets the timer for reauthentication on a given port. The re-authentication for the Supplicant is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no auth timeout reauth-period** command to reset the **reauth-period** parameter to the default value (3600 seconds).

Syntax `auth timeout reauth-period <1-4294967295>`

`no auth timeout reauth-period`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
timeout	Set a timeout parameter
reauth-period	Seconds between reauthorization attempts (default is 3600 seconds)
<1-4294967295>	Seconds

Default The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

Mode Interface mode

Example To set the reauthentication period to 1 day for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth timeout reauth-period
```

Validation Commands `show dot1x`
`show dot1x interface`

Related Commands `auth reauthentication`

auth timeout server-timeout

This command sets the timeout for the waiting response from the RADIUS server on a given port.

The **no auth timeout server-timeout** command resets the server-timeout to the default value (30 seconds).

Syntax `auth timeout server-timeout <1-65535>`
`no auth timeout server-timeout`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
timeout	Set a timeout parameter
server-timeout	Authentication server response timeout (default 30 seconds)
<1-65535>	Seconds

Default The server timeout for port authentication is 30 seconds.

Mode Interface mode

Example To set the server timeout to 120 seconds for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth timeout server-timeout
```

Validation Commands `show dot1x`
`show dot1x interface`

auth timeout supp-timeout

This command sets the timeout of the waiting response from the supplicant on a given port.

The **no auth timeout supp-timeout** command resets the supplicant timeout to the default (30 seconds).

Syntax `auth timeout supp-timeout <1-65535>`
`no auth timeout supp-timeout`

Parameter	Description
no	Negate a command or set its defaults
auth	Port Authentication
timeout	Set a timeout parameter
supp-timeout	Supplicant response timeout (default 30 seconds)
<1-65535>	Seconds

Default The supplicant timeout of port authentication is 30 seconds.

Mode Interface mode

Example To set the server timeout to 2 seconds for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth timeout supp-timeout 2
```

To reset the server timeout to the default (30 seconds) for interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth timeout supp-timeout
```

Validation Commands `show dot1x`
`show dot1x interface`

auth-mac enable

This command enables MAC based authentication on the interface specified in the Interface command mode.

Use the **no auth-mac enable** command to disable MAC based authentication on an interface.

Syntax `auth-mac enable`

`no auth-mac enable`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-mac</code>	MAC-Based Authentication
<code>enable</code>	Enables MAC authentication on the interface
<code>disable</code>	Disables MAC authentication on the interface

Default MAC authentication is disabled by default.

Mode Interface mode

Example To enable MAC authentication on interface port 1.0.2 , use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-mac enable
```

To disable MAC authentication on interface port 1.0.2 , use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-mac enable
```

Validation Commands `show auth-mac`
`show auth-mac interface`

Related Commands `aaa accounting auth-mac default`
`aaa authentication auth-mac`

auth-mac method

This command sets the type of authentication method for MAC authentication that is used with RADIUS on the interface specified in the Interface command mode.

The **no auth-mac method** command resets the authentication method used to the default method (EAP-MD5) as the RADIUS authentication method used by the MAC authentication.

Syntax `auth-mac method [eap-md5 | pap]`

`no auth-mac method`

Parameter	Description
no	Negate a command or set its defaults
auth-mac	MAC-Based Authentication
method	Authentic method (for RADIUS)
eap-md5	Enable EAP-MD5 of authentication method
pap	Enable PAP of authentication method

Default The mac authentication method is eap-md5.

Mode Interface mode

Example To set the MAC authentication method to pap on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-mac method pap
```

To set the MAC authentication method to default on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-mac method
```

Validation Commands `show auth-mac`
`show auth-mac interface`

auth-mac reauth-relearning

This command sets the MAC address learning of the supplicant to re-learning for re-authentication on the interface specified in the Interface command mode.

Use the **no auth-mac reauth-relearning** command to disable the auth-mac re-learning option.

Syntax `auth-mac reauth-relearning`
`no auth-mac reauth-relearning`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-mac</code>	MAC-Based Authentication
<code>reauth-relearning</code>	Relearning of MAC based Authentication

Default Re-learning for port authentication is disabled by default.

Mode Interface mode

Example To enable the re-authentication re-learning feature on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-mac reauth-relearning
```

Validation Commands `show auth-mac`
`show auth-mac interface`

auth-web enable

This command enables Web-based authentication in Interface mode on the interface specified.

Use the **no auth-web enable** command to disable Web-based authentication on an interface.

Syntax `auth-web enable`
`no auth-web enable`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web</code>	Web-based Authentication
<code>enable</code>	Enables Web-based authentication
<code>disable</code>	Disables Web-based authentication

Default Web authentication is disabled by default.

Mode Interface mode

Example To enable Web authentication on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-web enable
```

To disable Web authentication on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-web enable
```

Validation Commands `show auth-web`
`show auth-web interface`

Related Commands `aaa accounting auth-web default`
`aaa authentication auth-web`

auth-web forward

This command enables the web authentication packet forwarding feature on the interface specified.

This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

The **no auth-web forwarding** command disables or deletes the packet forwarding feature on the interface.

Syntax `auth-web forward {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}`
`no auth-web forward [arp|dhcp|dns|tcp <1-65535>|udp <1-65535>]`

Parameter	Description
no	Negate a command or set its defaults
auth-web	Web-Based Authentication
forward	Enable packet forwarding on a port
arp	Enable forwarding of ARP
dhcp	Enable forwarding of DHCP (67/udp)
dns	Enable forwarding of DNS (53/udp)
tcp	Enable forwarding of TCP specified port number
<1-65535>	TCP Port number
udp	Enable forwarding of UDP specified port number
<1-65535>	UDP Port number

Default Packet forwarding for port authentication is disabled by default.

Mode Interface mode

Example To enable the arp forwarding feature on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-web forward arp
```

To add the tcp forwarding port 137 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-web forward tcp 137
```

To disable the ARP forwarding feature on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-web forward arp
```

To delete the tcp forwarding port 137 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-web forward tcp 137
```

To delete the all of tcp forwarding on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-web forward tcp
```

Validation `show auth-web`
Commands `show auth-web interface`

auth-web max-auth-fail

This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant fails more than has been set to the maximum number of authentication failures then login requests are refused during the quiet period.

The **no auth-web max-auth-fail** command resets the maximum number of authentication failures to the default value (3 authentication failures).

Syntax `auth-web max-auth-fail <0-10>`

`no auth-web max-auth-fail`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web</code>	Web-Based Authentication
<code>max-auth-fail</code>	The number of Web authentication failures that causes a transition to the HELD state for Web authentication.
<code><0-10></code>	Lock count specified

Default The **max-auth-fail** lock counter is set to 3 authentication failures by default.

Mode Interface mode

Example To set the lock count to 5 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-web max-auth-fail 5
```

To set the lock count to the default on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#no auth-web max-auth-fail
```

Validation Commands `show auth-web`
`show auth-web interface`

Related Commands `auth timeout quiet-period`

auth-web method

This command sets the authentication method of WEB authentication that is used with RADIUS on the interface specified.

The **no auth-web method** command sets the authentication method to PAP for the interface specified when Web authentication is also used with the RADIUS authentication method.

Syntax `auth-web method {eap-md5 | pap}`

`no auth-web method`

Parameter	Description
<code>auth-web</code>	Web-Based Authentication
<code>method</code>	Authentic method (for RADIUS)
<code>eap-md5</code>	Enable EAP-MD5 as the authentication method
<code>pap</code>	Enable PAP as the authentication method

Default The web authentication method is set to PAP by default.

Mode Interface mode

Example To set the web authentication method to eap-md5 on interface port 1.0.2, use the following commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.2
awplus(config-if)#auth-web method eap-md5
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server http-redirect

This command enables the HTTP redirect feature on every port on which web-based port authentication is enabled. When the HTTP redirect feature is enabled, any HTTP request received on an unauthorized port is redirected to the web authentication server automatically.

Use the **no auth-web-server http-redirect** command to disable the HTTP redirect feature.

Syntax `auth-web-server http-redirect`
`no auth-web-server http-redirect`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>http-redirect</code>	redirect http request to web authentication server

Default The HTTP redirect feature is enabled by default.

Mode Global Configuration mode

Example To disable the HTTP redirect feature, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server http-redirect
```

To re-enable the HTTP redirect feature, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server http-redirect
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ipaddress

This command sets the IP address for the web authentication server.

Use the **no auth-web-server ipaddress** command to delete the IP address for the web authentication server.

Syntax `auth-web-server ipaddress <ip-addr>`
`no auth-web-server ipaddress`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
ipaddress	Set local web authentication server address
<ip-addr>	web authentication server dotted decimal ip address (A.B.C.D format)

Default The web authentication server address on the system is not set by default.

Mode Global Configuration mode

Example To set the IP address 10.0.0.1 to the web authentication server, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the web authentication server, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ipaddress
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ping-poll enable

This command enables the ping polling to the supplicant that is authenticated by web authentication.

The **no auth-web-server ping-poll enable** command disables the ping polling to the supplicant that is authenticated by web authentication.

Syntax `auth-web-server ping-poll enable`
`no auth-web-server ping-poll enable`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>ping-poll</code>	Ping polling configuration commands
<code>enable</code>	Enable ping polling

Default The ping polling feature for web authentication is disabled by default.

Mode Global Configuration mode

Example To enable the ping polling feature for web authentication, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ping-poll enable
```

To disable the ping polling feature for web authentication, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ping-poll enable
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ping-poll failcount

This command sets a fail count for the ping polling feature when used with web authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no auth-web-server ping-poll failcount** command to resets the fail count for the ping polling feature to the default (5 pings).

Syntax `auth-web-server ping-poll failcount <1-100>`

`no auth-web-server ping-poll failcount`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
ping-poll	Ping polling configuration commands
failcount	Set the number of pings that is unanswered (default 5)
<1-100>	Count

Default The default failcount for ping polling is 5 pings.

Mode Global Configuration mode

Example To set the failcount of ping polling to 10 pings, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ping-poll failcount
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ping-poll interval

This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant is reachable.

Use the **no auth-web-server ping-poll interval** command to reset to the default period for ping polling (30 seconds).

Syntax `auth-web-server ping-poll interval <1-65535>`

`no auth-web-server ping-poll interval`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
ping-poll	Ping polling configuration commands
interval	Set ping polling interval (default 30 seconds)
<1-65535>	Seconds

Default The interval for ping polling is 30 seconds by default.

Mode Global Configuration mode

Example To set the interval of ping polling to 60 seconds, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ping-poll interval
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ping-poll reauth-fresh

This command modifies the **reauth-fresh** parameter for the web-authentication feature. The **reauth-fresh** parameter specifies whether a re-authentication timer is reset and when the response from supplicant is received.

Use the **no auth-web-server ping-poll reauth-fresh** command to reset the **reauth-fresh** parameter to the default setting (disabled).

Syntax `auth-web-server ping-poll reauth-fresh`
`no auth-web-server ping-poll reauth-fresh`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>ping-poll</code>	Ping polling configuration commands
<code>reauth-fresh</code>	Enable reauthentication period updating when the response from supplicant is received

Default The **reauth-fresh** parameter is disabled by default.

Mode Global Configuration mode

Examples To enable the **reauth-fresh** timer; use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ping-poll reauth-fresh
```

To disable the **reauth-fresh** timer; use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ping-poll reauth-fresh
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server ping-poll timeout

This command modifies the ping poll **timeout** parameter for the web authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no auth-web-server ping-poll timeout** command to reset the timeout of ping polling to the default (1 second).

Syntax `auth-web-server ping-poll timeout <1-30>`

`no auth-web-server ping-poll timeout`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
ping-poll	Ping polling configuration commands
timeout	Set response waiting time (default 1 sec)
<1-30>	Seconds

Default The default timeout for ping polling is 1 second.

Mode Global Configuration mode

Example To set the timeout of ping polling to 2 seconds, use the command:

```
awplus#configure terminal
awplus(config)#auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus#configure terminal
awplus(config)#no auth-web-server ping-poll timeout
```

Validation Commands `show auth-web`
`show auth-web interface`

auth-web-server port

This command sets the HTTP port number for the web authentication server. Use the **no auth-web-server port** command to reset the HTTP port number to the default value (80). Specify a TCP port number in the range 1-65535 using the **auth-web-server port** command.

Syntax `auth-web-server port <port_num>`
`no auth-web-server port`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>port</code>	local web authentication server port number
<code><port_num></code>	Set the local web authentication server port within the TCP port number range <1-65535>

Default The web authentication server HTTP port number is set to 80 by default.

Mode Global Configuration mode

Example To set the HTTP port number 8080 for the web authentication server, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server port 8080
```

To reset to the default HTTP port number 80 for the web authentication server, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server port 1.15.9.6
```

Validation Commands `show auth-web`
`show auth-web-server`

auth-web-server redirect-url

This command sets a URL for supplicant authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no auth-web-server redirect-url** command to delete the URL string set previously.

Syntax `auth-web-server redirect-url <url>`

`no auth-web-server redirect-url`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
redirect-url	jump to the URL after the supplicant is authorized
<url>	URL (hostname or dotted IP notation)

Default The redirect URL for the web authentication server feature is not set by default (null).

Mode Global Configuration mode

Example To enable and set redirect a URL string **www.alliedtelesis.com** for the web authentication server, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server redirect-url www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server redirect-url
```

Validation Commands `show auth-web`
`show auth-web-server`

Related Commands `auth-web-server http-redirect`

auth-web-server session-keep

This command enables the session-keep feature to jump to the original URL after being authorized by web authentication.

Use the **no auth-web-server session-keep** command to disable the session keep feature.

Syntax `auth-web-server session-keep`
`no auth-web-server session-keep`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>session-keep</code>	jump to the requested URL after being authorized by web authentication

Default The session-keep feature is disabled by default.

Mode Global Configuration mode

Example To enable the session-keep feature, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server session-keep
```

Validation Commands `show auth-web`
`show auth-web-server`

auth-web-server ssl

This command enables HTTPS functionality for the web authentication server feature.

Use the **no auth-web-server ssl** command to disable HTTPS functionality for the web authentication server.

Syntax `auth-web-server ssl`
`no auth-web-server ssl`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>auth-web-server</code>	web authentication server configuration commands
<code>ssl</code>	Enable ssl web authentication server access

Default HTTPS functionality for the web authentication server feature is disabled by default.

Mode Global Configuration mode

Example To enable HTTPS functionality for the web authentication server feature, use the following commands:

```
awplus#configure terminal
awplus(config)#auth-web-server ssl
```

To disable HTTPS functionality for the web authentication server feature, use the following commands:

```
awplus#configure terminal
awplus(config)#no auth-web-server ssl
```

**Validation
Commands** `show auth-web`
`show auth-web-server`

auth-web-server sslport

This command sets the HTTPS port number for the web authentication server feature. Specify a TCP port number in the range 1-65535 using the **auth-web-server sslport** command.

Use the **no auth-web-server sslport** command to reset the HTTPS port number to the default port number (443) for the web authentication server feature.

Syntax `auth-web-server sslport <1-65535>`

`no auth-web-server sslport`

Parameter	Description
no	Negate a command or set its defaults
auth-web-server	web authentication server configuration commands
sslport	local web authentication server ssl port number
<1-65535>	Set the local web authentication server port within the TCP port number range <1-65535>

Default The HTTPS port number for the web authentication server feature is set to 443 by default.

Mode Configuration mode

Example To set the HTTPS port number to 4433 for the web authentication server, use the command:

```
awplus#configure terminal
awplus(config)#auth-web-server sslport 4433
```

To reset the HTTPS port number for the web authentication server to the default (443), use the command:

```
awplus#configure terminal
awplus(config)#no auth-web-server sslport
```

Validation Commands `show auth-web`
`show auth-web-server`

show auth-mac diagnostics

This command shows MAC authentication diagnostics for the specified interface (optional).

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax show auth-mac diagnostics [interface <*ifrange*>]

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
diagnostics	Diagnostics
interface	Specify an interface to show
< <i>ifrange</i> >	Interface range

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing authentication diagnostics for port 1.0.12:

```
awplus#show auth-mac diagnostics interface port1.0.12
```

```
Authentication Diagnostics for interface port1.0.12
```

```
Supplicant address: 00d0.59ab.7037
  authEnterConnecting: 2
  authEaplogoffWhileConnecting: 1
  authEnterAuthenticating: 2
  authSuccessWhileAuthenticating: 1
  authTimeoutWhileAuthenticating: 1
  authFailWhileAuthenticating: 0
  authEapstartWhileAuthenticating: 0
  authEaplogoggWhileAuthenticating: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
BackendResponses: 2
BackendAccessChallenges: 1
BackendOtherrequestToSupplicant: 3
BackendAuthSuccess: 1
```

show auth-mac interface

This command shows the status for MAC based authentication on the specified interface.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** parameter to show the supplicant state for the specified interface.

Syntax `show auth-mac interface <ifrange>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]`

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
interface	Specify an interface to show
<ifrange>	Interface range
diagnostics	Diagnostics
sessionstatistics	Session statistics
statistics	Statistics
supplicant	Supplicant
<brief>	Brief summary of supplicant state

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing MAC based authentication status for port 1.0.12:

```
awplus#show auth-mac interface port1.0.2
```

```
% Port-Control not configured on port1.0.2
```

See the sample output below showing MAC authentication diagnostics for port 1.0.12:

```
awplus#show auth-mac interface port1.0.12 diagnostics
```

```
Authentication Diagnostics for interface port1.0.12
```

```
Supplicant address: 00d0.59ab.7037
authEnterConnecting: 2
authEaplogoffWhileConnecting: 1
authEnterAuthenticating: 2
authSuccessWhileAuthenticating: 1
authTimeoutWhileAuthenticating: 1
authFailWhileAuthenticating: 0
authEapstartWhileAuthenticating: 0
authEaplogoggWhileAuthenticating: 0
authReauthsWhileAuthenticated: 0
authEapstartWhileAuthenticated: 0
authEaplogoffWhileAuthenticated: 0
BackendResponses: 2
BackendAccessChallenges: 1
BackendOtherrequestToSupplicant: 3
BackendAuthSuccess: 1
```

See the sample output below showing authentication session statistics for port 1.0.12:

```
awplus#show auth-mac interface port1.0.12 sessionstatistics
```

Authentication session statistics for interface port1.0.12

```
session user name: manager
session authentication method: Remote server
session time: 19440 secs
session terminat cause: Not terminated yet
```

To view MAC authentication statistics for port 1.0.12 issue the command:

```
awplus#show auth-mac interface port1.0.12 statistics
```

To show the MAC authenticated supplicant on interface port1.0.12 issue the command:

```
awplus#show auth-mac interface port1.0.12 supplicant
```

show auth-mac sessionstatistics

This command shows authentication session statistics for the specified interface.

Syntax `show auth-mac sessionstatistics [interface <ifranger>]`

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
sessionstatistics	Session statistics
interface	Specify an interface to show
<ifranger>	Interface range

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing MAC authentication session statistics for port 1.0.12:

```
awplus#show auth-mac sessionstatistics interface port1.0.12
Authentication session statistics for interface port1.0.12
  session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet
```

show auth-mac statistics interface

This command shows the authentication statistics for the specified interface.

Syntax `show auth-mac statistics [interface <ifranger>]`

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
statistics	Statistics
interface	Specify an interface to show
<ifranger>	Interface range

Mode Exec mode and Privileged Exec mode

Example To show MAC authentication statistics for port 1.0.12 issue the command:

```
awplus#show auth-mac statistics interface port1.0.12
```

show auth-mac supplicant

This command shows the supplicant state when MAC authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-mac supplicant [<macadd>] [brief]`

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
supplicant	Specify a supplicant to show
<macadd>	Mac (hardware) address of the Supplicant Entry format is HHHH.HHHH.HHHH (hexadecimal)
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example To show the MAC authenticated supplicant for MAC address 00d0.59ab.7037 issue the command:

```
awplus#show auth-mac supplicant 00d0.59ab.7037
```

show auth-mac supplicant interface

This command shows the supplicant state for the MAC authenticated interface. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-mac supplicant [interface <ifrange>] [brief]`

Parameter	Description
show	Show running system information
auth-mac	MAC-Based Authentication
supplicant	Specify a supplicant to show
interface	Specify an interface to show
<ifrange>	Interface range
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example To show the MAC authenticated supplicant on the interface port 1.0.12 issue the command:

```
awplus#show auth-mac supplicant interface port1.0.12
```

To show brief summary output for the MAC authenticated supplicant issue the command:

```
awplus#show auth-mac supplicant brief
```

show auth-web

This command shows authentication information for Web-based authentication.

If you specify the optional **all** parameter then this command also displays all authentication information for each interface available on the switch.

Syntax `show auth-web [all]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
all	All

Mode Exec mode and Privileged Exec mode

Example See the below example showing all Web authentication information:

```
awplus#show auth-web all
```

```
802.1X Port-Based Authentication Disabled  
MAC-based Port Authentication Disabled  
WEB-based Port Authentication Disabled
```

show auth-web diagnostics

This command shows Web authentication diagnostics for the specified interface (optional).

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax `show auth-web diagnostics [interface <ifrangle>]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
diagnostics	Diagnostics
interface	Specify an interface to show
<ifrangle>	Interface range

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing authentication diagnostics for port 1.0.12:

```
awplus#show auth-web diagnostics interface port1.0.12
```

```
Authentication Diagnostics for interface port1.0.12
  Supplicant address: 00d0.59ab.7037
    authEnterConnecting: 2
    authEaplogoffWhileConnecting: 1
    authEnterAuthenticating: 2
    authSuccessWhileAuthenticating: 1
    authTimeoutWhileAuthenticating: 1
    authFailWhileAuthenticating: 0
    authEapstartWhileAuthenticating: 0
    authEaplogoggWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
```

Related Commands [show dot1x interface](#)

show auth-web interface

This command shows the status for Web based authentication on the specified interface.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** parameter to show the supplicant state for the specified interface.

Syntax `show auth-web interface <ifrange>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
interface	Specify an interface to show
<ifrange>	Interface range
diagnostics	Diagnostics
sessionstatistics	Session statistics
statistics	Statistics
supplicant	Supplicant
brief	Brief summary of supplicant state

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing the Web based authentication status for port 1.0.12:

```
awplus#show auth-web interface port1.0.2
```

```
% Port-Control not configured on port1.0.2
```

See the sample output below showing Web authentication diagnostics for port 1.0.12:

```
awplusshow auth-web interface port1.0.12 diagnostics
Authentication Diagnostics for interface port1.0.12
  Supplicant address: 00d0.59ab.7037
    authEnterConnecting: 2
    authEaplogoffWhileConnecting: 1
    authEnterAuthenticating: 2
    authSuccessWhileAuthenticating: 1
    authTimeoutWhileAuthenticating: 1
    authFailWhileAuthenticating: 0
    authEapstartWhileAuthenticating: 0
    authEaplogoggWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
```

See the sample output below showing Web authentication session statistics for port 1.0.12:

```
awplus#show auth-web interface port1.0.12 sessionstatistics
```

```
Authentication session statistics for interface port1.0.12
  session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet
```

To view Web authentication statistics for port 1.0.12 issue the command:

```
awplus#show auth-web statistics interface port1.0.12
```

To show the Web authenticated supplicant on interface port1.0.12 issue the command:

```
awplus#show auth-web interface port1.0.12 supplicant
```

show auth-web sessionstatistics

This command shows authentication session statistics for the specified interface.

Syntax `show auth-web sessionstatistics [interface <ifrangle>]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
sessionstatistics	Session statistics
interface	Specify an interface to show
<ifrangle>	Interface range

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing Web authentication session statistics for port 1.0.12:

```
awplus#show auth-web sessionstatistics interface port1.0.12
```

```
Authentication session statistics for interface port1.0.12
  session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet
```

show auth-web statistics interface

This command shows the authentication statistics for the specified interface.

Syntax `show auth-web statistics interface <ifrang>`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
statistics	Statistics
interface	Specify an interface to show
<ifrang>	Interface range

Mode Exec mode and Privileged Exec mode

Example To show Web authentication statistics for port 1.0.12 issue the command:

```
awplus#show dot1x statistics interface port1.0.12
```

show auth-web supplicant

This command shows the supplicant state when Web authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-web supplicant [<macadd>] [brief]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
supplicant	Specify a supplicant to show
<macadd>	Mac (hardware) address of the Supplicant Entry format is HHHH.HHHH.HHHH (hexadecimal)
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example To show Web authenticated supplicant information on the switch issue the command:

```
awplus#show auth-web supplicant
```

To show brief summary output for the Web authenticated supplicant on the switch issue the command:

```
awplus#show auth-web supplicant brief
```

show auth-web supplicant interface

This command shows the supplicant state for the Web authenticated interface. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-web supplicant interface <ifrang> [brief]`

Parameter	Description
show	Show running system information
auth-web	Web-Based Authentication
supplicant	Specify a supplicant to show
interface	Specify an interface to show
<ifrang>	Interface range
brief	Brief summary of the Supplicant state

Mode Exec mode and Privileged Exec mode

Example To show the Web authenticated supplicant on the interface port 1.0.12 issue the command:

```
awplus#show auth-web supplicant interface port1.0.12
```

To show brief summary output for the Web authenticated supplicant the command:

```
awplus#show auth-web supplicant brief
```

show auth-web-server

This command shows the web authentication server configuration and status on the switch.

Syntax show auth-web-server

Parameter	Description
show	Show running system information
web-auth-server	web authentication server

Mode Exec mode and Privileged Exec mode

Example See the sample output below showing web authentication server status using this command:

```
awplus#show auth-web-server
```

```
Web authentication server
  Server status: enabled
  Server address: --
  HTTP Port No: 80
  Security: enabled
  Certification: default
  SSL Port No: 443
  Redirect URL:
  HTTP Redirect: disabled
  Session keep: disabled
  PingPolling: disable
  PingInterval: 30
  Timeout: 1
  FailCount: 5
  ReauthFresh: disabled
```

BGP commands

show bgp memory maxallocation

This command displays the maximum percentage of total memory that maybe allocated to the BGP routing process.

Syntax `show bgp memory maxallocation`

Parameter	Description
<code>show</code>	Show running system information
<code>bgp</code>	Border Gateway Protocol (BGP)
<code>memory</code>	Memory information
<code>maxallocation</code>	Maximum percentage of RAM allocated to daemons

Mode Privileged Exec Mode

Example To display the the maximum amount of memory BGP may allocate for its routing management, use the command:

```
awplus#show bgp memory maxallocation
      BGP maximum RAM allocation is 100%
```

show debugging bgp

Use this command to display the BGP debugging option set.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token. .

Syntax `show debugging bgp`

Mode Privileged Exec mode

Usage This is a sample output from the `show debugging bgp` command.

```
awplus#show debugging bgp

BGP debugging status:
  BGP debugging is on
  BGP events debugging is on
  BGP updates debugging is on
  BGP fsm debugging is on
```

Examples

```
awplus#show debugging bgp
```

show ip bgp prefix-list

Use this command to display routes matching the prefix-list.

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 bgp prefix-list <list>
show ip bgp ipv4 <prefix> prefix-list <list>

Parameter	Description
<list>	Specifies the name of the IP prefix list.
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.
<prefix>	{multicast unicast}
unicast	Specifies a IPv4 unicast address family. This is the default option.
multicast	Specifies a IPv4 multicast address family.

Mode Privileged Exec mode and Exec mode

Examples

```
awplus#show ip bgp prefix-list mylist
```

show ip bgp quote-regexp

Use this command to display routes matching the AS path regular expression in quotes.

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 bgp quote-regexp <expression>

Parameter	Description
<expression>	Specifies a regular-expression to match the BGP AS paths

Mode Privileged Exec mode and Exec mode

Examples

```
awplus#show ip bgp quote-regexp "myexpression"
```

show ip protocols bgp

Use this command to display BGP process parameters and statistics.

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 protocols bgp

Mode Exec mode and Privileged Exec mode

Output [Figure 0-1: Example output from the show ip protocols bgp command](#)

```
Routing Protocol is "bgp 100"
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Default local-preference applied to incoming route is 100
  Redistributing:
  Neighbor(s):
  Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut Weight
  10.10.10.1                unicast
```

Examples To display BGP process parameters and statistics, use the command:

```
awplus#show ip protocols bgp
```

Dynamic Host Configuration Protocol (DHCP) commands

ip dhcp-relay max-message-length

This command applies when the switch is acting as a *DHCP relay* and Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its 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.

Syntax `ip dhcp-relay max-message-length <548-1472>`

Parameter	Description
<code>ip dhcp-relay</code>	A device that forwards DHCP packets between a DHCP client and a DHCP server, usually located on a different network.
<code>max-message-length</code>	The maximum length of the DHCP message (in bytes) including the option 82 fields.
<code><548-1472></code>	The maximum DHCP message length (this is the message header plus the inserted DHCP option fields) Default: 1400
<code>no</code>	The no form of this command sets the maximum message length to its default of 1400 bytes.

Mode Interface mode

Usage Where a DHCP relay (that has option 82 insertion enabled) receives a *request* packet from a *DHCP client*, it will append the *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 option 82 data, the DHCP relay will increase the packet size to accommodate the option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP relay will drop the packet.

Note: Before setting this command, you must first run the `ip dhcp-relay agent option` command. This will allow the option 82 fields to be appended.

Examples To set the maximum DHCP message length to 1200 for packets arriving in interface `vlan7`, use the command:

```
awplus(config)#interface vlan7
awplus(config-if)#ip dhcp-relay max-message-length 1200
```

Related Commands `service dhcp-relay`

File management commands

copy current-software

This command copies the AlliedWare Plus™ OS software that the device has booted from to a destination file. Specify whether the destination is Flash or Card when saving the software to the local file system.

Syntax `copy current-software <destination-url>`

Parameter	Description
<code><destination-url></code>	The URL where you would like the current running-release saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file.

Mode Privileged Exec mode

Examples To copy the current software install the working directory with the name `my-release.rel`, use the command:

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

Related Commands [boot system](#)
[show boot](#)

copy debug

This command copies a specified debug file to a destination file. Specify whether the destination is Flash or Card when saving the software to the local file system.

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

Parameter	Description
<code><destination-url></code>	The URL where you would like the debug output saved.
<code><source-url></code>	The URL where the debug output originates.

Mode Privileged Exec mode

Examples To copy debug output to SD card with a filename `my-debug`, use the following command:

```
awplus#copy debug card:mydebug
```

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

Related Commands [delete debug](#)
[move debug](#)

delete

This command deletes files or directories.

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

Parameter	Description
<code>force</code>	Ignore nonexistent filenames and never prompt before deletion.
<code>recursive</code>	Remove the contents of directories recursively.
<code><url></code>	URL of the file to delete.

Mode Privileged Exec mode

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

Use this command to delete a specified debug output file.

Syntax `delete debug <source-url>`

Parameter	Description
<code><source-url></code>	The URL where the debug output originates.

Mode Privileged Exec mode

Examples To delete debug output, use the following command:

```
awplus#delete debug
```

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

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

move debug

This command moves a specified debug file to a destination debug file. Specify whether the destination is Flash or Card when saving the software to the local file system.

Syntax `move debug {<destination-url> | card | debug | flash | nvs | scp | tftp}
{<source-url> | card | debug | flash | nvs | scp | tftp}`

Parameter	Description
<code><destination-url></code>	The URL where you would like the debug output moved to.
<code><source-url></code>	The URL where the debug output originates.

Mode Privileged Exec mode

Examples To move debug output onto a SD card with a filename `my-debug`, use the following command:

```
awplus#move debug card:mydebug
```

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

Related Commands [copy debug](#)
[delete debug](#)

pwd

This command prints the current working directory.

Syntax `pwd`

Mode Privileged Exec mode

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

```
awplus#pwd
```

Related Commands [cd](#)

IGMP multicast commands

ip igmp ra-option (Router Alert)

With strict Router Alert (RA) option enabled, IGMP packets without RA options are ignored.

Use the **ip igmp ra-option** command to enable strict Router Alert (RA) option validation.

User the **no igmp ra-option** command to disable strict Router Alert (RA) option validation.

Syntax ip igmp ra-option
no ip igmp ra-option

Mode Interface mode

Default The default state of Router Alert (RA) validation is unset.

Usage This command applies to interfaces configured for IGMP, and IGMP Snooping.

Example

```
awplus#configure terminal
awplus(config)#interface vlan20
awplus(config-if)#ip igmp ra-option
```

ip igmp robustness-variable

Use this command to change the robustness variable value on an interface.

To return to the default value on an interface, use the **no** parameter with this command.

Syntax ip igmp robustness-variable <2-7>
no ip igmp robustness-variable

Mode Interface mode

Default The default robustness variable value is 2.

Usage This command applies to interfaces configured for IGMP, and IGMP Snooping.

Example

```
awplus#configure terminal
awplus(config)#interface vlan20
awplus(config-if)#ip igmp robustness-variable 3
```

show debugging igmp

Use this command to display the IGMP debugging option set.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token. .

Syntax show debugging igmp

Mode Privileged Exec mode

Usage This is a sample output from the show debugging igmp command.

```
awplus#show debugging igmp

awplus#debug igmp all
awplus#show debugging igmp
IGMP Debugging status:
  IGMP Decoder debugging is on
  IGMP Encoder debugging is on
  IGMP Events debugging is on
  IGMP FSM debugging is on
  IGMP Tree-Info-Base (TIB) debugging is on
```

Examples

```
awplus#show debugging igmp
```

IP addressing and protocols commands

debug ip packet interface

The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.

- The required *interface* placeholder following the optional **interface** 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.
- If the optional **address** keyword is specified then only packets with the specified IP address as specified in the *ip-address* placeholder are shown in the output.
- If the optional **verbose** keyword is specified then more of the packet is shown in the output.
- If an optional **hex** keyword is specified then the output for the packet is shown in hex.
- If the optional **arp** keyword is specified then ARP packets are shown in the output.
- If the optional **udp** keyword is specified then UDP packets are shown in the output.
- If the optional **tcp** keyword is specified then TCP packets are shown in the output.
- If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no debug ip interface** command disables the **debug ip interface** command.

Syntax

```
debug ip packet interface {<interface-name>|all}
    [address <ip-address>|verbose|hex|arp|udp|tcp|icmp]
no debug ip packet interface [<interface-name>]
```

Parameter	Description
interface-name	Specify a single layer 3 interface name (not a range of interfaces)
all	Specify all layer 3 interfaces on the switch.
ip-address	(A.B.C.D format) Specify an IPv4 address.
verbose	Specify verbose to output more of the IP packet.
hex	Specify hex to output the IP packet in hexadecimal.
arp	Specify arp to output ARP protocol packets.
udp	Specify udp to output UDP protocol packets.
tcp	Specify tcp to output TCP protocol packets.
icmp	Specify icmp to output ICMP protocol packets.

Mode Privileged Exec mode and Global Configuration mode

Example To turn on ARP packet debugging on VLAN 1, use the command:

```
awplus#debug ip packet interface vlan1 arp
```

To turn on all packet debugging on all interfaces on the switch, use the command:

```
awplus#debug ip packet interface all
```

To turn on TCP packet debugging on VLAN 1 and IP address 192.168.2.4, use the command:

```
awplus#debug ip packet interface vlan1 address 192.168.2.4 tcp
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus#no debug ip packet interface
```

To turn off IP packet interface debugging on interface VLAN 2, use the command:

```
awplus#no debug ip packet interface vlan2
```

ip irdp holdtime

This command sets the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

The **no** form sets the holdtime back to the default of 1800 seconds.

Syntax ip irdp holdtime <0-9000>
no ip irdp holdtime <0-9000>

Parameter	Description
<0-9000>	The holdtime value in seconds of addresses advertised. Default: 1800

Mode Interface mode

Default The IRDP holdtime is set to 1800 seconds (30 minutes) by default.

Example To set the holdtime value of addresses advertised on **vlan2** to 4000 seconds, use the command:

```
awplus#configure terminal
awplus(config)#interface vlan2
awplus(config-if)#ip irdp holdtime 4000
```

To set the holdtime value of addresses advertised on **vlan2** back to default, use the command:

```
awplus#configure terminal
awplus(config)#interface vlan2
awplus(config-if)#no ip irdp holdtime
```

Related Commands [show ip irdp interface](#)

Link aggregation commands

debug lacp

Use this command to enable all LACP troubleshooting functions.

Use the **no** parameter with this command to disable this function.

Syntax `debug lacp {all|cli|event|packet|sync|timer}`
`no debug lacp {all|cli|event|cli|packet|sync|timer}`

Parameter	Description
all	Turn on all debugging for LACP.
event	Specifies debugging for LACP events.
cli	Specifies debugging for CLI messages. Echoes commands to the console.
packet	Specifies debugging for LACP packets. Echoes packet contents to the console.
synch	Specified debugging for LACP synchronization. Echoes synchronization to the console.
timer	Specifies debugging for LACP timer. Echoes timer expiry to the console.

Mode Privileged Exec mode and Global Configuration mode

Usage This command with the **all** parameter turns on complete LACP debug information.

```
awplus#debug lacp all
awplus#show debugging lacp
LACP debugging status:
LACP timer debugging is on
LACP timer-detail debugging is on
LACP cli debugging is on
LACP packet debugging is on
LACP event debugging is on
LACP sync debugging is on
```

Examples

```
awplus#debug lacp
awplus#debug lacp all
```

Related Commands `show debugging mstp`

Local RADIUS server commands

attribute

Use the **attribute** command to show defined RADIUS attributes or configure defined RADIUS attributes. You cannot define RADIUS attribute names and must select one from a defined list.

When used with the **help** parameter the **attribute** command displays a list of standard and vendor specific valid RADIUS attributes that are supported by the Local RADIUS server:

If an attribute name is specified with the **name** parameter, then the **attribute** command displays a list of predefined attribute names. Note that you may only use the defined RADIUS attribute names and not define your own RADIUS attribute names.

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.

Syntax

```
attribute help
attribute [<name>] help
attribute <name> <value>
```

Parameter	Description
attribute	Set RADIUS attribute
<value>	RADIUS attribute value
<name>	RADIUS attribute name
help	Display a list of available attribute types

Mode RADIUS Server Group mode

Example To check a list of all available defined RADIUS attribute names, use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group Admin
awplus(config-radsrv-group)#attribute help
```

To get help for valid RADIUS User Group Admin attribute values with the attribute Service-Type, use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group Admin
awplus(config-radsrv-group)#attribute Service-Type help
```

```
Service-Type : integer (Integer number)
Pre-defined values :
  Administrative-User (6)
  Authenticate-Only (8)
  Authorize-Only (17)
  Callback-Administrative (11)
  Callback-Framed-User (4)
  Callback-Login-User (3)
  Callback-NAS-Prompt (9)
  Call-Check (10)
  Framed-User (2)
  Login-User (1)
  NAS-Prompt-User (7)
  Outbound-User (5)
```

To define the attribute name `Service-Type` with Administrative User (6) to the RADIUS User Group `Admin`, use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group Admin
awplus(config-radsrv-group)#attribute Service-Type 6
```

To delete the attribute '`Service-Type`' from the RADIUS User Group '`Admin`', use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group Admin
awplus(config-radsrv-group)#no attribute Service-Type
```

To show all defined attributes for the RADIUS User Group '`Admin`', use the following commands. Note that you may only use the defined RADIUS attributes and not define them. A list of vendor specific attributes displays after the list of defined RADIUS attributes.

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group Admin
awplus(config-radsrv-group)#attribute help
```

authentication

This command allows you to enable specified authentication methods on Local RADIUS server.

Use the **no** parameter to disable specified authentication methods on Local RADIUS server.

Syntax `authentication {mac|eapmd5|eaptls|peap}`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>authentication</code>	RADIUS authentication configuration commands
<code>mac</code>	Enable MAC authentication method
<code>eapmd5</code>	Enable EAP-MD5 authentication method
<code>eaptls</code>	Enable EAP-TLS authentication method
<code>peap</code>	Enable EAP-PEAP authentication method

Default All authentication methods are enabled by default.

Mode RADIUS Server mode

Example The following commands enable EAP-MD5 authentication methods on 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
```

Validation Commands `show radius local-server statistics`

Related Commands `server enable`

group

This command allows you to create a Local RADIUS Server user group, and also enables the Local RADIUS Server User Group Configuration Mode.

The **no group** command allows user to delete Local RADIUS Server user group.

Syntax `group <user-group-name>`
`no group <user-group-name>`

Parameter	Description
no	Negate a command or set its defaults
group	RADIUS user group configuration commands
<user-group-name>	User group name string

Mode RADIUS Server mode

Example The following command creates user group NormalUsers.

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#group NormalUsers
```

The following command deletes user group NormalUsers.

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#no group NormalUsers
```

Validation Commands `show radius local-server user`

crypto pki enroll local

Use this command to obtain a system certificate from the Local CA (Certificate Authority).

Use the **no crypto pki enroll local** command to delete system certificates created by a Local CA (Certificate Authority).

Syntax `crypto pki enroll local`
`no crypto pki enroll local`

Parameter	Description
no	Negate a command or set its defaults
crypto	Security specific commands
pki	Public Key Infrastructure (PKI) commands
enroll	Enroll to specified trustpoint
local	Local Certificate Authority

Default The system certificate is not available until this command is issued.

Mode Global Configuration mode

Example The following command obtains the system certificate from the Local CA (Certificate Authority).

```
awplus#configure terminal
awplus(config)#crypto pki enroll local
```

The following command deletes the system certificate created by the Local CA (Certificate Authority).

```
awplus#configure terminal
awplus(config)#no crypto pki enroll local
```

Related Commands [crypto pki trustpoint local](#)
[group](#)

crypto pki enroll local local-radius-all-users

This command allows to obtain certificates for the user registered to a Local RADIUS server certificate from the Local CA (Certificate Authority).

Syntax `crypto pki enroll local local-radius-all-users`

Parameter	Description
<code>crypto</code>	Security specific commands
<code>pki</code>	Public Key Infrastructure (PKI) commands
<code>enroll</code>	Enroll to specified trustpoint
<code>local</code>	Local Certificate Authority
<code>local-radius-all-users</code>	Certificates for all users registered to Local RADIUS server

Default The key for Local RADIUS server users does not exist until created using this command.

Mode Global Configuration mode

Example The following command obtains the Local RADIUS server certificates for the user from the Local CA (Certificate Authority).

```
awplus#configure terminal
awplus(config)#crypto pki enroll local local-radius-all-users
```

Validation Commands `show crypto pki certificates`

Related Commands `crypto pki trustpoint local`

crypto pki enroll local user

This command allows you to obtain a local user certificate from the Local CA (Certificate Authority).

Use the **no crypto pki enroll local user** command to delete user certificates created by the Local CA (Certificate Authority).

Syntax `crypto pki enroll local user <user-name>`
`no crypto pki enroll local user <user-name>`

Parameter	Description
no	Negate a command or set its defaults
crypto	Security specific commands
pki	Public Key Infrastructure (PKI) commands
enroll	Enroll to specified trustpoint
local	Local Certificate Authority
user	Certificates for user
<user-name>	User name description

Default The user certificate does not exist until created.

Mode Global Configuration mode

Example The following command obtains Tom's certificate from the Local CA (Certificate Authority).

```
awplus#configure terminal
awplus(config)#crypto pki enroll local user Tom
```

The following command deletes Tom's certificates created by the Local CA (Certificate Authority):

```
awplus#configure terminal
awplus(config)#no crypto pki enroll local user Tom
```

Validation Commands `show crypto pki certificates`

Related Commands `crypto pki trustpoint local`

crypto pki export local pem

This command allows you to export the certificate associated with the Local CA to a PEM format file.

Syntax `crypto pki export local pem url <url>`

Parameter	Description
<code>crypto</code>	Security specific commands
<code>pki</code>	Public Key Infrastructure (PKI) commands
<code>export</code>	Export certificates
<code>local</code>	Local Certificate Authority
<code>pem</code>	Export Local CA certificate to PEM format file
<code>url</code>	Specify destination url
<code><url></code>	Url string

Mode Global Configuration mode

Example The following command exports the Local CA certificate to a PEM format file.

```
awplus#configure terminal
awplus(config)#crypto pki export local pem url tftp://192.168.1.1/
cacert.pem
```

Related Commands `crypto pki enroll local`

crypto pki export local pkcs12

This command allows you to export a specified certificate to a PKCS12 format file.

This command cannot be used for exporting certificates for the local system.

Syntax `crypto pki export local pkcs12 <user-name> <destination-url>`

Parameter	Description
<code>crypto</code>	Security specific commands
<code>pki</code>	Public Key Infrastructure (PKI) commands
<code>export</code>	Export certificates
<code>local</code>	Local Certificate Authority
<code>pkcs12</code>	Export user certificate to PKCS12 format file
<code><user-name></code>	User name
<code><destination-url></code>	Destination url string

Mode Global Configuration mode

Example The following commands exports a certificate named **client** to a PKCS12 format file.

```
awplus#configure terminal
awplus(config)#crypto pki export local pkcs12 client tftp://
192.168.1.1/cacert.pem
```

To export Tom's certificate to PKSC12 format file, use the commands:

```
awplus#configure terminal
awplus(config)#crypto pki export local pksc12 Tom tftp://192.168.1.1/
tom.pfx
```

Related Commands `crypto pki enroll local`

crypto pki trustpoint local

This command allows you to declare the Local CA (Certificate Authority) as the trustpoint that system uses. The ca-trustpoint configuration mode is available after this command is issued.

The **no crypto pki trustpoint local** command allows you to delete all information and certificates associated with Local CA as the trustpoint.

Syntax `crypto pki trustpoint local`
`no crypto pki trustpoint local`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>crypto</code>	Security specific commands
<code>pki</code>	Public Key Infrastructure (PKI) commands
<code>trustpoint</code>	Declare trustpoint
<code>local</code>	Local Certificate Authority

Default Local CA is not a trustpoint.

Mode Global Configuration mode

Examples Use the following commands to declare the Local CA as the trustpoint.

```
awplus#configure terminal
awplus(config)#crypto pki trustpoint local
```

Use the the following command to delete all information and certificates associated with the Local CA.

```
awplus#configure terminal
awplus(config)#no crypto pki trustpoint local
```

To create a client certificate for all users registered to the Local Radius Server, use the following commands:

```
awplus(config)#crypto pki trustpoint local
awplus(ca-trust-point)#exit
awplus(config)#crypto pki enroll local alternative
```

Validation Commands `show crypto pki trustpoints`

Related Commands `crypto pki enroll local`

debug crypto

This command enables Public Key Infrastructure (PKI) debugging. When PKI debugging is enabled, the PKI module starts generating diagnostic messages to the system log.

Use the **no debug crypto** command to disable Public Key Infrastructure (PKI) debugging. When PKI debugging is disabled, the PKI module stops generating diagnostic messages to the system log.

Syntax `debug crypto pki`
`no debug crypto pki`

Parameter	Description
no	Negate a command or set its defaults
debug	Debugging functions (see also 'undebug')
crypto	Security Specific
pki	Public Key Infrastructure (PKI)

Default PKI debugging is disabled by default

Mode Privileged Exec mode

Example To enable the PKI debugging facility, use the command:

```
awplus#debug crypto pki
```

To disable the PKI debugging facility, use the command:

```
awplus#no debug crypto pki
```

nas

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 nas** command to remove a NAS client from the list of devices that are allowed to send authentication requests to the Local RADIUS Server.

Syntax `nas <ip-address> key <nas-keystring>`
`no nas <ip-address>`

Parameter	Description
no	Negate a command or set its defaults
nas	RADIUS NAS configuration commands
<ip-address>	RADIUS NAS IP address
key	Specify the shared key for NAS
<nas-keystring>	NAS shared keystring

Mode RADIUS server mode

Example 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
```

Validation Commands `show radius local-server nas`

radius-server local

Use this command to navigate to the Local RADIUS server configuration mode (config-radsrv) from the Global Configuration mode (config).

Syntax radius-server local

Parameter	Description
radius-server	RADIUS server
local	Local RADIUS server commands

Mode Global Configuration mode

Example Local RADIUS Server commands are available from config-radsrv configuration mode. To change mode from Exec mode to the Local RADIUS Server mode (config-radsrv) enter:

```
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)#
```

server auth-port

This command allows you to change the UDP port number for Local RADIUS server authentication.

The **no server auth-port** command allows you to reset the RADIUS server authentication port back to the default.

Syntax `server auth-port <1-65535>`
`no server auth-port`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>server</code>	RADIUS local server configuration commands
<code>auth-port</code>	Set local server's authentication port
<code><1-65535></code>	UDP port number

Default The default Local RADIUS server UDP authentication port number is 1812.

Mode RADIUS Server mode

Example The following command sets RADIUS server authentication port to 10000.

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#server port 10000
```

The following command resets 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 port
```

server enable

This command enables Local RADIUS server. The Local RADIUS server feature is started immediately when this command is issued.

The **server enable** command disables Local RADIUS server. When this command is issued, Local Radius server stops operating.

Syntax server enable
no server enable

Parameter	Description
no	Negate a command or set its defaults
server	RADIUS local server configuration commands
enable	Enable local server

Default The Local RADIUS server is disabled by default and must be enabled for use with this command.

Mode RADIUS Server mode

Examples To enable Local RADIUS server issue the following command in RADIUS server Mode:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#server enable
```

To disable Local RADIUS server issue the following command in RADIUS server Mode:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#no server enable
```

Validation Commands show radius local-server statistics

Related Commands server auth-port

show crypto pki certificates

This command enables you to display certificate information.

Syntax `show crypto pki certificates [local-ca|local|<certificate-name>]`

Parameter	Description
show	Show running system information
crypto	Security Specific
pki	Public Key Infrastructure (PKI)
certificates	Certificate information
local-ca	Local CA certificate
local	Local system certificate
<certificate-name>	Certificate name

Mode Privileged Exec mode

Example The following command displays Local CA (Certificate Authority) certificate information.

```
awplus#show crypto pki certificates local-ca
```

The following command displays Local System certificate information.

```
awplus#show crypto pki certificates local
```

The following command displays Tom's local certificate information.

```
awplus# show crypto pki certificates Tom
```

The following command displays information of all certificates.

```
awplus#show crypto pki certificates
```

Output

```
Certificate: Local CA
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
Validity
Not Before: Mar 20 08:46:29 2008 GMT
Not After : Mar 15 08:46:29 2028 GMT
Subject: O=Allied-Telesis, CN=AlliedwarePlusCA

Certificate: Local System
Version: 3 (0x2)
Serial Number: 4 (0x4)
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
Validity
Not Before: Mar 20 09:03:01 2008 GMT
Not After : Mar 18 09:03:01 2018 GMT
Subject: O=Allied-Telesis, CN=AlliedwarePlusSystem
```

Output Description

Parameter	Description
Certificate	Certificate name
Version	Protocol version
Serial Number	Serial number of the certificate
Signature Algorithm	Algorithm used for the certificate signature
Issuer	Subject of issuer creating the certificate
Validity	Validity period
Subject	Subject of the certificate

Related Commands `crypto pki enroll local`

show crypto pki certificates local-radius-all-users

This command enables you to display certificate information for Local RADIUS server users.

Syntax `show crypto pki certificates local-radius-all-users`

Parameter	Description
show	Show running system information
crypto	Security Specific
pki	Public Key Infrastructure (PKI)
certificates	Certificate information
local-radius-all-users	All Local RADIUS server users

Mode Privileged Exec mode

Example The following command displays information of all Local RADIUS server user certificates.

```
awplus#show crypto pki certificates local-radius-all-users
```

Output

```
Certificate: Alice
Not exist.
Certificate: Tom
Version: 3 (0x2)
Serial Number: 13 (0xd)
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
Validity
Not Before: Mar 22 07:17:15 2008 GMT
Not After : Mar 20 07:17:15 2018 GMT
Subject: O=Allied-Telesis, CN=Tom
```

Output Description

Parameter	Description
Certificate	Certificate name
Version	Protocol version
Serial Number	Serial number of the certificate
Signature Algorithm	Algorithm used for the certificate signature
Issuer	Subject of issuer creating the certificate
Validity	Validity period
Subject	Subject of the certificate

Related Commands `crypto pki enroll local local-radius-all-users`

show crypto pki certificates user

This command enables you to display certificate information for Local RADIUS server users.

Syntax `show crypto pki certificates user [<user-name>]`

Parameter	Description
show	Show running system information
crypto	Security Specific
pki	Public Key Infrastructure (PKI)
certificates	Certificate information
user	All Local RADIUS server users
<user-name>	user name

Mode Privileged Exec mode

Example The following command displays Tom's certificate information.

```
awplus#show crypto pki certificates user Tom
```

Output

```
Certificate: Tom
Version: 3 (0x2)
Serial Number: 13 (0xd)
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
Validity
Not Before: Mar 22 07:17:15 2008 GMT
Not After : Mar 20 07:17:15 2018 GMT
Subject: O=Allied-Telesis, CN=Tom
```

Output Description

Parameter	Description
Certificate	Certificate name
Version	Protocol version
Serial Number	Serial number of the certificate
Signature Algorithm	Algorithm used for the certificate signature
Issuer	Subject of issuer creating the certificate
Validity	Validity period
Subject	Subject of the certificate

Related Commands `crypto pki enroll local user`

show crypto pki trustpoints

This command enables you to display trustpoint information.

Syntax `show crypto pki trustpoints`

Parameter	Description
show	Show running system information
crypto	Security Specific
pki	Public Key Infrastructure (PKI)
trustpoints	Trustpoint information

Mode Privileged Exec mode

Example The following command displays trustpoint information.

```
awplus#show crypto pki trustpoint
```

Output

```
Trustpoint local:
Subject Name:
CN = AlliedwarePlusCA
o = Allied-Telesis
Serial Number:0C
```

Output Description

Parameter	Description
Subject Name	CA certificate subject
Serial Number	Current serial number of CA

Related Commands `crypto pki enroll local`

show radius local-server group

This command displays information about Local RADIUS server user group.

Syntax `show radius local-server group [<user-group-name>]`

Parameter	Description
show	Show running system information
radius	Radius protocol
local-server	Local RADIUS server
group	RADIUS user group
<user-group-name>	User group name string

Mode Privileged Exec mode

Example The following command displays Local RADIUS server user group information.

```
awplus#show radius local-server group
```

Output

Group-Name	Vlan

NetworkOperators	ManagementNet
NormalUsers	CommonNet

Output Description

Parameter	Description
Group-Name	Group name
Vlan	VLAN name assigned to the group

Related Commands `group`

show radius local-server nas

This command displays information about NAS registered to Local RADIUS server.

Syntax `show radius local-server nas [<ip-address>]`

Parameter	Description
show	Show running system information
radius	RADIUS protocol
local-server	Local RADIUS server
nas	RADIUS NAS
<ip-address>	Specify NAS IP address for show output

Mode Privileged Exec mode

Example The following command displays NAS information.

```
awplus#show radius local-server nas
```

Output

```
NAS-Address  Shared-Key
-----
127.0.0.1    awplus-local-radius-server
```

Output Description

Parameter	Description
NAS-Address	IP address of NAS
Shared-Key	Shared key used for RADIUS connection

Related Commands `nas`

show radius local-server statistics

This command displays statistics about Local RADIUS server.

Syntax show radius local-server statistics

Parameter	Description
show	Show running system information
radius	RADIUS protocol
local-server	Local RADIUS server
statistics	Statistics

Mode Privileged Exec mode

Examples The following command displays Local RADIUS server statistics.

```
awplus#show radius local-server statistics
```

Output

```
awplus#show radius local-server statistics
Server status : Run (administrative status is enable)
Enabled methods: MAC EAP-MD5 EAP-TLS EAP-PEAP

Successes                :0                Unknown NAS                :0
Unknown username         :0                Invalid passwords         :0
Invalid packet from NAS:0                Internal Error             :0
Unknown Error            :0

NAS : 127.0.0.1
Successes                :0                Shared key mismatch       :0
Unknown username         :0                Invalid passwords         :0
Unknown RADIUS message  :0                Unknown EAP message       :0
Unknown EAP auth type   :0                Corrupted packet          :0
```

show radius local-server user

This command displays information about Local RADIUS server user.

Syntax show radius local-server user <user-name> format csv

Parameter	Description
show	Show running system information
radius	RADIUS protocol
local-server	Local RADIUS server
user	RADIUS user
<user-name>	User name
format	File format
csv	Comma separated value format

Mode Privileged Exec mode

Example The following command displays Local RADIUS server user information.

```
awplus#show radius local-server user Tom format csv
```

Output

```
true,"NetworkOperators","Tom",
"abcd",0,2099/01/
01,1,"","","ManagementNet",false,3600,false,0,"",false,"
```

Related Commands user (RADIUS server)

show radius local-server user

This command displays information about Local RADIUS server user.

Syntax show radius local-server user [*<user-name>*]

Parameter	Description
show	Show running system information
radius	RADIUS protocol
local-server	Local RADIUS server
user	RADIUS user
<i><user-name></i>	User name

Mode Privileged Exec mode

Example The following command displays all Local RADIUS server user information.

```
awplus#show radius local-server user
```

Output

User-Name	Password	Group	Vlan
Alice	1234	NormalUsers	CommonNet
Tom	abcd	NetworkOperators	ManagementNet

Example The following command displays Local RADIUS server user information for a user named Tom.

```
awplus#show radius local-server user
```

Output

User-Name	Password	Group	Vlan
Tom	abcd	NetworkOperators	ManagementNet

Output Description

Parameter	Description
User-Name	User name
Password	User password
Group	Group name assigned to the user
Vlan	VLAN name assigned to the user

Related Commands group
user (RADIUS server)

user (RADIUS server)

This command allows you to register a user to the Local RADIUS server.

The **no user** command allows you to delete a user from the Local RADIUS server.

Syntax `user <radius-user-name> password <user-password>`
`[group <user-group-name>]`
no user <radius-user-name>

Parameter	Description
no	Negate a command or set its defaults
user	RADIUS user database configuration commands
<radius-user-name>	RADIUS user name
password	Specify the password for user
<user-password>	User password string
group	Specify the group for user
<user-group-name>	User group name string

Mode RADIUS Server mode

Example The following command adds 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 command adds user Tom to 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 command removes user Tom from Local RADIUS server:

```
awplus#configure terminal
awplus(config)#radius-server local
awplus(config-radsrv)#no user Tom
```

Validation Commands `show radius local-server user`

Related Commands `group`

vlan (RADIUS server)

This command allows user to set the VLAN ID or name for the Local RADIUS server user group.

The VLAN information is used by the Network Switch device dynamic VLAN feature. The **no vlan** command allows user to clear VLAN ID or name for the Local RADIUS server user group.

Syntax `vlan <vlan-id>`

`no vlan`

Parameter	Description
<code>no</code>	Negate a command or set its defaults
<code>vlan</code>	Set VLAN information
<code><vlan-id></code>	VLAN information string

Default VLAN information is not set by default.

Mode RADIUS Server Group mode

Example 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
```

Validation Commands `show radius local-server user`

Related Commands `group`

OSPF commands

maximum-area

Use this command to set the maximum number of OSPF areas.

Use the **no maximum-area** command to set the maximum number of OSPF areas to the default value. The default value for the maximum number of OSPF areas is 4294967294.

Syntax `maximum-area <1-4294967294>`
`no maximum-area`

Parameter	Description
<code><1-4294967294></code>	Specify the maximum number of OSPF areas.

Mode Router OSPF mode

Usage Use this command in router OSPF mode to specify the maximum number of OSPF areas.

Examples The following example sets the maximum number of OSPF areas to 2:

```
awplus#configure terminal
awplus(config)#router ospf 100
awplus(config-router)#maximum-area 2
```

The following example removes the maximum number of OSPF areas and resets to default:

```
awplus#configure terminal
awplus(config)#router ospf 100
awplus(config-router)#no maximum-area
```

ospf restart grace-period

Use this command to configure the Grace Period for restarting OSPF.

Use the **no** parameter with this command to revert to default.

Syntax `ospf restart grace-period <1-1800>`
`no ospf restart grace-period <1-1800>`

Parameter	Description
<1-1800>	Specifies the grace period in seconds.

Mode Global Configuration mode

Usage Use this command to enable the OSPF Graceful Restart feature.

Examples `awplus#configure terminal`
`awplus(config)#ospf restart grace-period 250`

ospf restart helper

Use this command to configure the **helper** behavior for the OSPF Graceful Restart feature.

Use the **no** parameter with this command to revert to the default.

Syntax `ospf restart helper`
`{max-grace-period <1-1800> | never | only-reload | only-upgrade}`
`no ospf restart helper [max-grace-period]`

Parameter	Description
never	Local Policy to never to act as Helper
only-reload	Help only on software reloads
only-upgrade	Help only on software upgrades
max-grace-period	Help only if received grace-period is less than this value

Mode Global Configuration mode

Examples `awplus#configure terminal`
`awplus(config)#ospf restart helper only-reload`

show ip protocols ospf

Use this command to display OSPF process parameters and statistics.

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 protocols ospf

Mode Exec mode and Privileged Exec mode

Output Figure 0-2: Example output from the show ip protocols ospf command

```

Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
    Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
    192.30.30.0/24
    192.40.40.0/24
  Routing Information Sources:
    Gateway         Distance         Last Update
  Distance: (default is 110)
  Address           Mask             Distance List
  
```

Examples To display OSPF process parameters and statistics, use the command:

```
awplus#show ip protocols ospf
```

PIM Sparse Mode commands

ip pim anycast-rp

Use the **ip pim anycast-rp** command to configure Anycast RP (Rendezvous Point) in a RP set.

Use the **no ip pim anycast-rp** command to remove the configuration set with **ip pim anycast-rp**.

Syntax

```
ip pim anycast-rp <anycast_rp_address> <member_rp_address>
ip pim anycast-rp <anycast_rp_address> [<member_rp_address>]
```

Parameter	Description
<anycast_rp_address>	<100-199> IP extended access-list.
<member_rp_address>	<2000-2699> IP extended access list (expanded range).

Mode Global Configuration mode

Usage Anycast is a network addressing and routing scheme where data is routed to the nearest or best destination as viewed by the routing topology. Compared to unicast with a one-to-one association between network address and network endpoint, and multicast with a one-to-many association between network address and network endpoint; anycast has a one-to-many association between network address and network endpoint. For anycast, each destination address identifies a set of receiver endpoints, from which only one receiver endpoint is chosen.

Anycast is often implemented using BGP to simultaneously advertise the same destination IP address range from many sources, resulting in packets address to destination addresses in this range being routed to the nearest source announcing the given destination IP address.

Use this command to specify the Anycast RP configuration in the Anycast RP set. Use the **no** parameter with this command to remove the Anycast RP configuration. Note that the member RP address is optional when using the **no** parameter to remove the Anycast RP configuration. removing the anycast RP address also removes the member RP address.

Example The following example shows how to configure the Anycast RP address with **ip pim anycast-**

```
awplus#configure terminal
awplus(config)#ip pim anycast-rp 1.1.1.1 10.10.10.10
```

rp:

The following example shows how to remove the Anycast RP in the RP set specifying only the anycast RP address with **no ip pim anycast-rp**, but not specifying the member RP address:

```
awplus#configure terminal
awplus(config)#no ip pim anycast-rp 1.1.1.1
```

ip pim bsr-border

Use the **ip pim bsr-border** command to prevent bootstrap router (BSR) messages from being sent or received through an interface. The BSR border is the border of the PIM domain.

Use the **no ip pim bsr-border** command to disable configuration set with **ip pim bsr-border**.

Syntax ip pim bsr-border
no ip pim bsr-border

Mode Interface mode

Usage When this command is configured on an interface, no PIM version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two PIM domains.

BSR messages should not be exchanged between different domains, because devices in one domain may elect Rendezvous Points (RPs) in the other domain, resulting in loss of isolation between the two PIM domains that would stop the PIM protocol from working as intended.

Example The following example configures the interface specified to be the PIM domain border:

```
awplus#configure terminal
awplus(config)#interface vlan2
awplus(config-if)#ip pim bsr-border
```

The following example removes the interface specified from the PIM domain border:

```
awplus#configure terminal
awplus(config)#interface vlan2
awplus(config-if)#no ip pim bsr-border
```

Quality of Service (QoS) commands

mls qos fabric-queue

Configures the scheduling algorithm for one or more fabric queues. If the scheduler is weighted round robin (WRR), a weighting can also be specified. You must specify at least one queue when setting this command.

The **no** variant of this command resets the scheduling algorithm for one or more input fabric queues. Default is priority.

Syntax `mls qos fabric-queue {[0][1][2][3]}{priority|wrr [weight <1-30>]}`
`no mls qos fabric-queue [0][1][2][3]Mode`

Parameter	Description
mls	Multi-Layer Switch(L2/L3)
qos	Quality of Service
fabric-queue	The one or more fabric queues being configured by this command
0, 1, 2, 3	fabric queues being configured
priority	Applies strict priority queue servicing to the selected queues
wrr	Applies weighted round robin queue servicing to the selected queues
weight	The weight for weighted round robin selection. Queues will then be serviced in proportion to their applied weights. Default is 1.
<1-30>	The weight value
no	Returns the selected ports to priority queueing

Mode Global Configuration mode

Usage Queues can be serviced in either priority sequence or a weighted round-robin sequence. By default all queues are set to priority servicing.

Priority Sequencing

In this mode the queue with the highest number, i.e. queue 3 will be emptied first, then queues 2, 1 and 0. Note that the lower queues will only be serviced if there is no data waiting in the higher numbered queues.

Weighted Round Robin Sequencing

In this mode the weighting that you assign to each queue will determine how often it is serviced with respect to the other WRR queues. For example, if queue 0 is configured with a weight of 5 and queue 1 is configured with a weight of 1, then queue 0 will be serviced 5 times more than queue 1. Setting all weights to the same value will therefore apply an unweighted round selection method.

Mixed Sequencing

If you configure the queues with a mix of priority queueing and WRR, the priority queues will be completely emptied, before the any WRR queue is serviced.

Examples To set the scheduler for fabric queues 0 and 1 to WRR and both have a weight of 5 use the command:

```
awplus#config terminal
awplus(config)#mls qos fabric-queue 0 1 wrr weight 5
```

To reset the scheduling algorithm for fabric-queues 0 and 1, use the command:

```
awplus#config terminal
awplus(config)#no mls qos fabric-queue 0 1
```

mls qos map fabric-queue

This command maps eight egress queues to four fabric queues. Note that when entering this command, you must supply a mapping for all eight egress queues.

Use the **no mls qos map fabric-queue** command to reset the fabric queue map. This table maps eight egress queues to four fabric queues. The default maps egress queues 0 and 1 to fabric queue 0, egress queues 2 and 3 to fabric queues 1, egress queues 4 and 5 to fabric queue 2 and egress queues 6 and 7 to fabric queue 3.

Syntax `mls qos map fabric-queue q0 q1 q2 q3 q4 q5 q6 q7`
`no mls qos map fabric-queue`

Parameter	Description
no	Negate a command or set its defaults
mls	Multi-Layer Switch(L2/L3)
qos	Quality of Service
map	Specify maps
fabric-queue	Modify the egress queue to fabric queue map
q0	Egress queue 0 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q1	Egress queue 1 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q2	Egress queue 2 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q3	Egress queue 3 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q4	Egress queue 4 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q5	Egress queue 5 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q6	Egress queue 6 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)
q7	Egress queue 7 (Select a value 0 to 3 to map this egress queue to one of the four fabric queues q0-q4)

Mode Global Configuration Mode

Examples This example maps egress queue 7 to fabric queue 3, egress queue 6 to fabric queue 2, egress queue 5 to fabric queue 1, and the rest of the egress queues to fabric queue 0. Use the command:

```
awplus#config terminal
awplus(config)#mls qos map fabric-queue 0 0 0 0 0 1 2 3
```

The following table shows how the queue mapping operates in the above example:

Egress Queue	0	1	2	3	4	5	6	7
Fabric Queue Mapping	0	0	0	0	0	1	2	3

To reset the fabric-queue map, use the command:

```
awplus#config terminal
awplus(config)#no mls qos map fabric-queue
```

mls qos map premark-dscp to

Configures the premark-dscp map. This is used when traffic is classified by a class-map that has trust DSCP configured. Based on a lookup DSCP, the map determines a new DSCP, COS, queue and bandwidth class for the traffic. If the set DSCP command has also been specified for that class-map, the set value is used for the lookup of the premark-dscp map. Otherwise the DSCP value in the packet is used for the lookup.

The **no** variant of this command resets the premark-dscp map to its defaults. This is used when traffic is classified by a class-map that has trust dscp configured. Based on a lookup DSCP, the map determines a new DSCP, COS, queue and bandwidth class for the traffic. If the set DSCP command has also been specified for that class-map, the set value is used for the lookup of the premark-dscp map. Otherwise the DSCP value in the packet is used for the lookup. If no DSCP is specified then all DSCP entries will be reset to their defaults.

Syntax

```
mls qos map premark-dscp <0-63> to {[new-dscp <0-63>]
[new-cos<0-7>] [new-queue <0-7>] [new-bandwidth-class{green|yellow|
red}]}
```

```
no mls qos map premark-dscp [<0-63>]
```

Parameter	Description
premark-dscp<0-63>	The DSCP value on ingress
new-dscp<0-63>	The DSCP value that the packet will have on egress. If unspecified, this value will remain the DSCP ingress value.
new-cos<0-7>	The CoS value that the packet will have on egress. If unspecified, this value will be set to zero.
new-bandwidth-class	Modify Egress Bandwidth-class. If unspecified, this value will be set to green.
green	Egress Bandwidth-class green (marked down Bandwidth-class)
yellow	Egress Bandwidth-class yellow (marked down Bandwidth-class)
red	Egress Bandwidth-class red (marked down Bandwidth-class)

Mode Global Configuration mode

Examples To set the entry for DSCP 1 to use a new DSCP of 2, a new CoS of 3, a new queue of 4 and a new bandwidth class of yellow, use the command:

```
awplus#config terminal
awplus(config)#mls qos map premark-dscp 1 to new-dscp 2 new-cos 3 new-queue 4 new-bandwidth-class yellow
```

To reset the entry for DSCP 1 use the command:

```
awplus#config terminal
awplus(config)#no mls qos map premark-dscp 1
```

mls qos map policed-dscp to

Configures the policed-dscp map. This is used when a policer is configured with an exceed action of 'policed-dscp-transmit'. Bandwidth-class is optional - if omitted, the changes will be applied to all bandwidth classes. At least one 'new' parameter must be specified.

Use the **no** variant to reset the policed-dscp map to its default. This is used when a policer is configured with an exceed action of 'policed-dscp-transmit'. Specifying DSCP and bandwidth-class is optional. If no DSCP is specified then all DSCP entries will be reset to their defaults. If no bandwidth-class is specified then all bandwidth-class entries will be reset to their defaults.

Syntax

```
mls qos map policed-dscp <existing-dscp> [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>][new-cos <0-7>][new-queue <0-7>][new-bandwidth-class {green|yellow|red}]}
```

```
no mls qos map policed-dscp [<new-dscp>] [bandwidth-class {green|yellow|red}]
```

Parameter	Description
map	Specify maps
policed-dscp	Modify the policed-DSCP map
<existing-dscp>	The value of the DSCP when it leaves the policer (meter) <0-63>
bandwidth-class	Bandwidth Class
green	Mark the packet as green
yellow	Mark the packet as yellow
red	Mark the packet as red
to	Change the value to:
new-dscp	Modify Egress DSCP
<0-63>	Egress DSCP value (marked down DSCP)
new-cos	Modify Egress CoS
<0-7>	Egress CoS value (marked down CoS)
new-queue	Modify Egress Queue
<0-7>	Egress Queue value (marked down Queue)
new-bandwidth-class	Modify Egress Bandwidth-class
green	Egress Bandwidth-class green (marked down Bandwidth-class)
yellow	Egress Bandwidth-class yellow (marked down Bandwidth-class)
red	Egress Bandwidth-class red (marked down Bandwidth-class)

Parameter	Description
no	Negate a command or set its defaults
mls	Multi-Layer Switch(L2/L3)
qos	Quality of Service
map	Specify map
policed-dscp	Reset the policed-DSCP map to its defaults
<0-63>	DSCP entry to reset
bandwidth-class	bandwidth class to reset
green	Green traffic
yellow	Yellow traffic
red	Red traffic

Mode Global Configuration mode

Example To set the entry at DSCP 2 to remark the policed green traffic to a new DSCP of 2, a new CoS of 3, and new queue of 4 and a new bandwidth class of yellow, use the command:

```
awplus#config terminal
awplus (config)#mls qos map policed-dscp 2
                    bandwidth-class green to new-dscp 5
                    new-cos 3 new-queue 4 new-bandwidth-class
                    yellow
```

set queue

Use this command to set a queue value to assign to classified traffic. This will override the default queue as configured by [mls qos queue command](#) but may be overridden by subsequent QoS mechanisms (such as remarking).

This command is not valid if the [trust dscp command](#) is set.

Syntax set queue <0-7>

Parameter	Description
set	Setting a new value in the packet
queue	Queue
<0-7>	Specify a new Queue value
no	Negate a command or set its defaults

Mode Policy Map Class

Example To set the queue to value 7 for all traffic classified as cmap1 and pmap1, use the command:

```
awplus#configure terminal
awplus (config)#policy-map pmap1
awplus (config-pmap)#class cmap1
awplus (config-pmap-c)#set queue 7
```

show class-map

Use this command to display the QoS class maps to define the match criteria to classify traffic.

Syntax `show class-map <class-map name>`

Parameter	Description
<code><class-map name></code>	name of the class map.

Mode Exec mode and Privileged Exec mode

Example

```
awplus#show class-map cmap1
CLASS-MAP-NAME: cmap1
Set IP DSCP: 56
Match IP DSCP: 7
```

storm-protection

Enables the Policy Based Storm Protection (such as QSP - QoS Storm Protection).

Syntax

```
storm-protection
no storm-protection
```

Parameter	Description
<code>storm-protection</code>	Policy-based storm protection
<code>no</code>	Negate a command or set its defaults

Mode Policy Map Class

Example To enable QSP on cmap2 in pmap2, use the commands:

```
awplus#policy-map pmap2
awplus(config-pmap)#class-map cmap2
awplus(config-pmap-c)#storm-protection
```

RADIUS commands

deadtime (Server Group)

Use this command to configure the **deadtime** parameter for the RADIUS server group. This command overrides the global dead-time configured by the [radius-server deadtime command](#).

The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is "dead". Note that a RADIUS server is considered "dead" if there is no response from the server within a defined time period.

Use the **no deadtime (Server Group) 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>no</code>	Negate a command or set its defaults
<code>deadtime</code>	Configure dead-time parameter
<code><0-1440></code>	Amount of time in minutes (default: 0)

Default The deadtime is set to 5 minutes by default.

Mode Server Group Configuration mode

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.

Example To configure the deadtime for 5 minutes for the RADIUS server group "GROUP1", use the command:

```
awplus(config)#aaa group server radius GROUP1
awplus(config-sg)#server 192.168.1.1
awplus(config-sg)#deadtime 5
```

To remove the deadtime configured for the RADIUS server group "GROUP1", use the command:

```
awplus(config)#aaa group server radius GROUP1
awplus(config-sg)#no deadtime
```

debug radius

This command enables RADIUS debugging.

- If **packet** is specified with **debug radius**, debugging for RADIUS packets is enabled.
- If **event** is specified with **debug radius**, debugging for RADIUS events is enabled.
- If **all** is specified with **debug radius**, all debugging options are enabled.
- If no option is specified with **debug radius**, all debugging options are enabled.

Use the **no debug radius** command to disable RADIUS debugging.

- If **packets** is specified with **no debug radius**, debugging for RADIUS packets is disabled.
- If **events** is specified with **no debug radius**, debugging for AAA events is disabled.
- If **all** is specified with **no debug radius**, all debugging options are disabled.
- If no option is specified with **no debug radius**, all debugging options are disabled.

Syntax `debug radius [packet|event|all]`

`no debug radius [packet|event|all]`

Parameter	Description
no	Negate a command or set its defaults
debug	Debugging functions (see also 'undebug')
radius	RADIUS protocol
packet	Packet trace
event	Event trace
all	Turn on all debugging

Default RADIUS debugging is disabled by default.

Mode Privileged Exec mode

Example 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
```

ip radius source-interface

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 will depend on the interface the packets leave by.

The **no ip radius source-interface** command removes the source interface configuration made by ip radius source-interface command. With no source interface configured the source IP address of outgoing RADIUS packets will depend on the interface the packets leave by.

Syntax ip radius source-interface {<interface>|<ipaddr>}
no ip radius source-interface

Parameter	Description
no	Negate a command or set its defaults
ip	Internet Protocol (IP)
radius	RADIUS configuration commands
source-interface	Set interface for source address in radius packets
<interface>	Interface name
<ipaddr>	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 mode

Usage Use this command to configure 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** version 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.

Example To configure all outgoing RADIUS packets to use the IP address of the interface "vlan1" for the source IP address, use the following commands:

```
awplus#configure terminal
awplus(config)#ip radius source-interface vlan1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus#configure terminal
awplus(config)#ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus#configure terminal
awplus(config)#no ip radius source-interface
```

server (Server Group)

This command adds a RADIUS server to a server group in Server-Group Configuration mode. The RADIUS server should be configured by the **radius-server host** command.

The server is appended to the server list of the group, and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before adding the new one.

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. 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 server** 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
no	Negate a command or set its defaults
server	Configure RADIUS server
<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 Authentication port number is 1812 and the Accounting port number is 1813 by default.

Mode Server Group Configuration mode

Usage The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the auth-port and acct-port parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

The server is appended to the server list of the group, and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before adding the new one.

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.

Example 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
```

show debugging radius

This command displays the current debugging status for the RADIUS servers.

Syntax show debugging radius

Parameter	Description
show	Show running system information
debugging	Debugging functions (see also 'undebug')
radius	RADIUS servers

Mode Privileged Exec mode

Examples To display the current debugging status of RADIUS servers, use the command:

```
awplus#show debug radius
```

```
RADIUS debugging status:  
  RADIUS event debugging is off  
  RADIUS packet debugging is off
```

show radius

This command displays the current RADIUS server configuration and status.

Syntax show radius

Parameter	Description
show	Show running system information
radius	RADIUS protocol

Mode Privileged Exec mode

Output Description

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. <ul style="list-style-type: none"> • Alive : the server is alive • Error : the service is not responding • Dead : the service 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.

Example To display the current status of RADIUS servers, use the command:

```
awplus#show radius
```

```
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
```

See the sample output below showing RADIUS client status and RADIUS configuration:

```
awplus#show radius
```

```
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
show radius local-server group
```

show radius statistics

This command shows the RADIUS client statistics for the switch.

Syntax show radius statistics

Parameter	Description
show	Show running system information
radius	RADIUS Server configuration and RADIUS status
statistics	RADIUS Server statistics

Mode Privileged Exec mode

Example See the sample output below showing RADIUS client statistics and RADIUS configuration:

```
awplus#show radius statistics

RADIUS statistics for Server: 150.87.18.89
  Access-Request Tx      : 5 - Retransmit           : 0
  Access-Accept Rx      : 1 - Access-Reject Rx      : 2
  Access-Challenge Rx   : 2
  Unknown Type          : 0 - Bad Authenticator     : 0
  Malformed Access-Resp : 0 - Wrong Identifier     : 0
  Bad Attribute         : 0 - Packet Dropped       : 0
  TimeOut               : 0 - Dead count           : 0
  Pending Request       : 0
```

RIP commands

rip restart grace-period

Use this command to change the grace period of RIP graceful restart.

Use the **no** parameter with this command to disable this function.

Syntax `rip restart grace-period <1-65535>`
 `no rip restart grace-period <1-65535>`

Mode Global Configuration mode

Usage Use this command to enable the `Graceful Restart` feature on the RIP process.
 Entering this command configures a grace period for RIP.

Example `awplus#configure terminal`
 `awplus(config)#rip restart grace-period 200`

Secure Shell (SSH) commands

ssh server authentication

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 ssh server authentication** 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.

Mode Global Configuration mode

Default Both RSA public-key authentication and password authentication are enabled by default.

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.

Example To enable **password** authentication for users connecting through SSH, use the commands:

```
awplus#configure terminal
awplus(config)#no ssh server authentication password
```

To enable **publickey** authentication for users connecting through SSH, use the commands:

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

SNMP commands

snmp-server source-interface

Use this command to specify the interface that SNMP traps or informs originate from. You cannot specify an interface that does not already have an IP address assigned to the interface.

Use the **no snmp-server source-interface** command to reset to the default source interface that SNMP traps or informs originate from (the Egress interface as sent from by default).

Syntax `snmp-server source-interface {traps|informs} <interface-name>`
`no snmp-server source-interface {traps|informs}`

Parameter	Description
no	Negate a command or set its defaults
snmp-server	Manage snmp server
source-interface	Enable SNMP traps
traps	SNMP traps
informs	SNMP informs
<interface-name>	Interface name (with an IP address already assigned)

Mode Global Configuration mode

Default By default the source interface is the Egress interface where traps or informs were sent from.

Usage An SNMP trap or inform sent from an SNMP server has the notification IP address of the interface where it was sent from. Use this command to monitor notifications from an interface.

Example To set the interface that SNMP informs originate from to port 1.0.2 for inform packets, use the following commands:

```
awplus#configure terminal
awplus(config)#snmp-server source-interface informs port1.0.2
```

To reset the interface to the default source interface (the Egress interface) that SNMP traps originate from for trap packets, use the following commands:

```
awplus#configure terminal
awplus(config)#no snmp-server source-interface traps
```

Validation Commands `show running-config`

Spanning tree commands

spanning-tree guard root

Use this command to enable the Root Guard feature for the port. The root guard feature disables reception of superior BPDUs.

Use this command for RSTP, STP or MSTP.

Use the **no** parameter with this command to disable the root guard feature for the port.

Syntax spanning-tree guard root
no spanning-tree guard root

Mode Interface mode

Usage The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Example

```
awplus#configure terminal
awplus(config)#interface port1.1.2
awplus(config-if)#spanning-tree guard root
```

show debugging mstp

Use this command to display the MSTP debugging option set.

To modify the lines displayed, use the | (output modifier token) ; to save the output to a file use the > output redirection token. .

Syntax show debugging mstp

Mode Privileged Exec mode

Usage This is a sample output from the show debugging mstp command.

```
awplus#debug mstp packet rx
awplus#show debugging mstp
MSTP debugging status:
MSTP receiving packet debugging is on
```

Examples

```
awplus#show debugging mstp
```

Stacking commands (SwitchBlade x908 only)

stack software-auto-synchronization

Enables the software auto-synchronization feature for a specific stack candidate¹.

1. A stack candidate is a switch that will attempt to join a stack.

Syntax stack <1-8> software-auto-synchronization
no stack <1-8> software-auto-synchronization

Parameter	Description
no	Negate a command or set its defaults
stack	Manage VCS feature
<1-8>	The ID of the stack candidate
software-auto-synchronization	Initiate the software version auto-synchronization process

Default All stack candidates¹ have the software-auto-synchronization feature enabled by default. Use the **no** form of this command to turn the feature off.

Mode Global Configuration mode

Usage This command is used to enable the software auto-synchronization feature for a specific stack member. When a new member joins a stack and has a software release that is different to the other stack members, the software auto-synchronization feature will copy the master's software release onto the new member. If the auto-upgrade feature is not enabled, then the new member will not remain in the stack.

Note that the software auto-synchronization feature may also result in the new stack member downgrading its software release if the master is running an older software version.

Examples To turn on the auto-copy feature on stack member 2, which is turned off previously, use the commands:

```
awplus#configure terminal
awplus(config)#stack 2 software-auto-synchronization
```

Validation Command awplus#show stack

Related Commands show stack

Switching commands

clear mac address-table dynamic

Use this command to clear the filtering database of all entries learned for a given MAC address, interface or VLAN.

Syntax `clear mac address-table dynamic [address <mac-address>|vlan <vid>|interface <port>]`

Parameter	Description
interface	Filtering database entries for the given port.
<vid>	when filtering database entries are cleared based on VLANs. Value range is 1-4094.
<port>	The port from which address entries will be cleared. This can be a single port, such as port1.1.4, a static channel group, such as sa3, or an LACP channel group, such as po4.
<mac-address>	The mac address to be cleared from the database.

Mode Privileged Exec mode

Usage Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries. Compare this usage and operation with the **clear mac address-table static** command.

Examples This example shows how to clear all dynamically learned filtering database entries for all interfaces, addresses, VLANs.

```
awplus#clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through switch operation for a given MAC address.

```
awplus#clear mac address-table dynamic address 0202.0202.0202
```

Related Commands [clear mac address-table static](#)
[show mac address-table](#)

clear mac address-table static

Use this command to:

- clear all filtering database entries configured through CLI (static)
- clear all static database entries based on a mac address

Syntax `clear mac address-table static [address <mac-address>|vlan <vid>|
interface <port>]`

Parameter	Description
vlan	Filtering database entries for the given VLAN.
interface	Filtering database entries for the given port.
<vid>	The VLAN IDs to be cleared from the database. Value range is 1-4094.
<port>	The port from which address entries will be cleared. This can be a single port, such as port1.1.4, a static channel group, such as sa3, or an LACP channel group, such as po4.
<mac-address>	The mac address to be cleared from the database.

Mode Privileged Exec mode

Usage Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI. Compare this usage with **clear mac address-table dynamic**.

Examples This example shows how to clear all filtering database entries configured through the CLI.

```
awplus#clear mac address-table static
```

This example shows how to clear all filtering database entries for a given interface configured through the CLI.

```
awplus#clear mac address-table static interface port1.1.3
```

This example shows how to clear filtering database entries filtering database entries configured through the CLI for a given mac address.

```
awplus#clear mac address-table static address 0202.0202.0202
```

platform bist

This command performs a self test on the switch. This command tests the ASIC (Application Specific Integrated Circuit) memory.

Syntax `platform bist instance {<0-127>|all} [full]`

Parameter	Description
instance	ASIC (Application Specific Integrated Circuit) instance
<0-127>	ASIC instance number
all	All platform instances
full	Run full BIST tests

Mode Privileged Exec mode

Examples To run the full built in self test for all memory in the ASIC on the switch, issue the command:

```
awplus#platform bist instance all full
```

Related Commands [show platform bist](#)

platform control-plane-prioritization rate

The CPU protection feature ensures that different traffic types can share the CPU effectively.

Use this command to set the maximum traffic rate on the CPU port to limit the CPU getting overloaded with unnecessary data packets that may result in poor performance of the control plane, for example, CLI console lock up or control packet loss following a broadcast storm.

The default rate limiting value is set to transmit the packets to the CPU at 60 Mbps. The CPU port uses the WRR (Weighted Round Robin) scheduler with appropriate weights assigned.

Use the **no platform control-plane-prioritization** command to restore the rate limiting on the CPU port to the default value of 60 Mbps. Note only integer values are accepted for rate limits.

Set the rate to 0 using **platform control-plane prioritization rate** to disable CPU protection.

Syntax `platform control-plane-prioritization rate <rate-limit>`

`no platform control-plane-prioritization rate`

Parameter	Description
<rate-limit>	<1-1000> Mbps to 1000 Mbps. Default is 60 Mbps.

Mode Global Configuration mode

Default 60 Mbps

Usage Confirming default settings:

Use **show platform** to confirm the default rate limit settings displayed with platform information:

```
awplus#show platform
Load Balancing                srt-dst-mac, src-dst-ip
Control-plane-prioritization Max 60 Mbps
Jumboframe support            off
Enhanced mode                  qos counters
Vlan-stacking TPID            0x8100
```

Disabling CPU protection:

To disable the CPU protection feature you can set the control plane prioritization rate to 0:

```
awplus#platform control-plane-prioritization 0
```

Then you can confirm the CPU protection feature has been disabled using **show platform**:

```
awplus#show platform
Load Balancing                srt-dst-mac, src-dst-ip
Control-plane-prioritization Max 0 Mbps
Jumboframe support            off
Enhanced mode                  qos counters
Vlan-stacking TPID            0x8100
```

Example To set the maximum traffic rate on the CPU port to 10 Mbps issue the following command:

```
awplus(config)#platform control-plane-prioritization 10
```

Confirm the maximum traffic rate has been configured using the following **show** command:

```
awplus#show platform
Load Balancing                srt-dst-mac, src-dst-ip
Control-plane-prioritization Max 10 Mbps
Jumboframe support            off
Enhanced mode                  qos counters
Vlan-stacking TPID            0x8100
```

Reset the maximum traffic rate on the CPU port to 60 Mbps using the following **no** command:

```
awplus(config)#no platform control-plane-prioritization
```

platform load-balancing

This command enables the use of packet fields in the channel load balancing algorithm.

Use the **no platform load-balancing** command to disable the use of packet fields in the channel load balancing algorithm.

The load balancing algorithm determines the member port of a trunk group when the packet is destined for a port within a trunk group. The load balancing algorithm also determines the flow group to which a packet belongs when the packet is associated with a traffic class that has flow groups enabled.

When Layer 4 (**src-dst-port**) is enabled then Layer 3 (**src-dst-ip**) header information is also used to hash traffic to a trunked port. When traffic is routed at Layer 3 to a trunk group then only Layer 3 header information is used to hash traffic to the ports in the trunk group, irrespective of whether **src-dst-mac**, **src-dst-ip** or **src-dst-port** is enabled.

Syntax

```
platform load-balancing {src-dst-mac|src-dst-ip|src-dst-port}
[src-dst-mac|src-dst-ip|src-dst-port]

no platform load-balancing {src-dst-mac|src-dst-ip|src-dst-port}
[src-dst-mac|src-dst-ip|src-dst-port]
```

Parameter	Description
src-dst-mac	Include Source and Destination MAC data
src-dst-ip	Include Source and Destination IP data
src-dst-port	Include Source and Destination TCP/UDP port data

Mode Global Configuration mode

Default The default is **src-dst-mac** and **src-dst-ip**

Example To set the load balancing algorithm to include layer 4 port information:

```
awplus(config)#platform load-balancing src-dst-port
```

To set the load balancing algorithm to exclude layer 4 port information:

```
awplus(config)#no platform load-balancing src-dst-port
```

platform routingratio

Syntax `platform routingratio {ipv4only|ipv4andipv6}`

Description This command changes the amount of memory allocated to IPv4 routing tables relative to IPv6 routing tables.

The switching hardware contains memory that it uses to store tables of routes and nexthop addresses. IPv4 and IPv6 addresses have separate tables. This command adjusts the amount of memory allocated to the tables depending on whether they are for IPv4 or IPv6 addresses.

Parameter	Description
ipv4only	All memory resources are allocated to the IPv4 address tables.
ipv4andipv6	50% of memory resources are allocated to the IPv4 address tables, and 50% to IPv6 address tables.

Mode Global Configuration mode

Examples To set the route and nexthop tables to IPv4 only, use the command:

```
awplus(config)#platform routingratio ipv4only
```

platform prbs

Use this command to perform a PRBS (Pseudo-Random Bit Stream) test on the system. This test sends a PBRS bidirectionally to and from every fabric port on the switch.

Syntax `platform prbs [duration <seconds>]`

Parameter	Description
duration	Duration of test.
<seconds>	The duration period, in seconds.

Mode Privileged Exec mode

Example To perform a PBRS for 5 minutes on the switch, use the following command:

```
awplus#platform prbs duration 300
```

show mac address-table thrash-limit

Use this command to display the current thrash limit set for all interfaces on the device.

Syntax show mac address-table thrash-limit

Mode Exec mode and Privileged Exec mode

Example To display the current , use the command:

```
awplus#show mac address-table thrash-limit
```

```
% Thrash-limit 7 movements per second
```

Related Commands [mac address-table thrash-limit](#)

thrash-limiting

MAC address thrashing occurs when MAC addresses move rapidly between one or more ports or trunks, for example, due to a network loop.

Thrash limiting enables you to apply actions to a port when thrashing is detected. It is supported on all port types and also on aggregated ports.

Limiting Actions

There are several different thrash actions that you can apply to a port when thrashing is detected. These actions are:

- **learnDisable**
Address learning is temporarily disabled on the port.
- **portDisable**
The port is logically disabled. Traffic flow is prevented, but the link remains up. The device at the other end does not notice that the port has changed status, and the link LEDs at both ends stay on.
- **linkDown**
The port is physically disabled and the link is down. This is equivalent to entering the **shutdown** command.
- **vlanDisable**
The port is disabled only for the VLAN on which thrashing has occurred. It can still receive and transmit traffic for any other VLANs of which it is a member.

When a MAC address is thrashing between two ports, one of these ports (the first to cross its thrashing threshold) is disabled. All other ports on the device will then have their threshold counters reset.

To set a thrash action for a port, use the **thrash-limiting** command.

To view the thrash action that is set for a port, use the **show interface switchport** command.

Re-enabling a port When a port is disabled, either completely or for a specific VLAN, it remains disabled until it is manually re-enabled in any of the following ways:

- by using SNMP
- by rebooting the switch or stack
- by specifying a thrash timeout value along with the thrash action
- via the CLI

This command sets and configures the thrash limit action that will be applied to any port on the switch when a thrashing condition is detected. The thrash-limiting timeout specifies the time, in seconds, for which the thrash action is employed.

Syntax `thrash-limiting {[action {learn-disable|link-down|port-disable|vlan-disable|none}]} [timeout{<0-86400>}]}`
`no thrash-limiting {action|timeout}`

Parameter	Description
<code>thrash-limiting</code>	set mac address thrash limiting
<code>action</code>	the mac thrashing detected action. The default is <code>vlan-disable</code> .
<code>learn-disable</code>	disable mac address learning
<code>link-down</code>	block all traffic on an interface - link down
<code>port-disable</code>	block all traffic on an interface - link remains up
<code>vlan-disable</code>	block all traffic on a vlan Note that setting this parameter will also enable ingress filtering.
<code>none</code>	no thrash action
<code>timeout</code>	set the duration for the thrash action
<code><0-86400></code>	the duration of the applied thrash action - in seconds. The default is 7 seconds.
<code>no</code>	sets either the selected thrash limiting action or its timeout to the default value.

Mode Interface Mode

Example To set the action to learn disable, use the command:

```
awplus(config-if)#thrash-limiting action learn-disable
```

To set the thrash limiting timeout to 5 seconds, use the command:

```
awplus(config-if)#thrash-limiting timeout 5
```

To set the thrash limiting action to its default, use the command:

```
awplus(config-if)#no thrash-limiting action
```

To set the thrash limiting timeout to its default, use the command:

```
awplus(config-if)#no thrash-limiting timeout
```

System configuration and monitoring commands

debug nsm

This command specifies a set of debug options for use by Allied Telesis authorized service personnel only. Use this command to specify the debug options set for the routing manager.

Syntax debug nsm [all|events]
no debug nsm [all|events]

Mode Privileged Exec mode and Global Configuration mode

Related Commands [show debugging nsm](#)

debug nsm packet

This command specifies a set of debug options for use by Allied Telesis authorized service personnel only. Use this command to specify the debug options for the nsm packet.

Syntax debug nsm packet [recv|send] [detail]
no debug nsm packet

Mode Privileged Exec mode and Global Configuration mode

Related Commands [show debugging nsm](#)

max-fib-routes

Use this command to set the maximum number of fib (forwarding information base) routes, excluding static routes. Note that static routes are set and reset using **max-static-routes**.

Use the **no max-fib-routes** command to set the maximum number of fib routes to the default value of 4294967294 fib routes.

Syntax max-fib-routes <1-4294967294>
no max-fib-routes

Mode Global Configuration mode

Mode The default number of fib routes is the maximum number of fib routes (4294967294).

Example To reset the maximum number of forwarding information base routes issue the command:

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

max-static-routes

Use this command to set the maximum number of static routes, excluding fib routes. Note that fib routes are set and reset using **max-fib-routes**.

Use the **no max-static-routes** command to set the maximum number of static routes to the default value of 1000 static routes.

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

Mode Global Configuration mode

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

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

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

show system interrupts

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 switch.

Syntax `show system interrupts`

Parameter	Description
show	Show running system information
system	System properties
interrupts	interrupts per IRQ

Mode Exec mode and Privileged Exec mode

Output [Figure 0-3: Example output from the show system interrupts command](#)

```
awplus>show system interrupts
      CPU0
  1:      2  CPM2 SIU  Level Enabled  0    i2c-mpc
  2:     145  CPM2 SIU  Level Enabled  0    spi-mpc
 77:      0  OpenPIC  Level Enabled  0    enet_tx
 78:      2  OpenPIC  Level Enabled  0    enet_rx
 82:      0  OpenPIC  Level Enabled  0    enet_error
 90:    5849  OpenPIC  Level Enabled  0    serial
 91:  2066672  OpenPIC  Level Enabled  0    i2c-mpc
 94:     147  OpenPIC  Level Enabled  0    cpm2_cascade
112:      5  OpenPIC  Edge  Enabled  0    phy_interrupt
114:   398714  OpenPIC  Level Enabled  0    mvPP
115:   26247  OpenPIC  Level Enabled  0    mvPP
119:      0  OpenPIC  Edge  Enabled  0    Power supply status
120:      0  OpenPIC  Edge  Enabled  0    Plugin XEM
BAD:      0
```

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

```
awplus#show system interrupts
```

Related Commands [show system environment](#)

show system pci device

Use this command to display the PCI devices on your switch.

Syntax `show system pci device`

Parameter	Description
show	Show running system information
system	System properties
pci	PCI information
device	PCI device list

Mode Exec mode and Privileged Exec mode

Output [Figure 0-4: 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]
```

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

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

Related Commands `show system environment`
`show system pci tree`

show system pci tree

Use this command to display the PCI tree on your switch.

Syntax `show system pci tree`

Parameter	Description
show	Show running system information
system	System properties
pci	PCI information
tree	PCI tree view

Mode Exec mode and Privileged Exec mode

Output [Figure 0-5: Example output from the show system pci tree command](#)

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

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

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

Related Commands [show system environment](#)
[show system pci device](#)

Trigger commands

trigger activate

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 mode.

Usage This command manually activates a trigger without the normal trigger conditions being met. The trigger is activated even if it is configured as inactive. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

Examples To manually activate trigger 12 use the command:

```
awplus#trigger activate 12
```

Related Commands [show trigger](#)
[trigger](#)

VRRP commands

virtual-ip

Use this command to set the virtual IP address for the VRRP session. This is the IP address of the virtual router that end hosts set as their default gateway.

Use the **no** parameter with this command to disable this feature.

Syntax `virtual-ip A.B.C.D master`
`virtual-ip A.B.C.D backup`
`no virtual-ip`

Parameter	Description
<i>A.B.C.D</i>	The virtual IP address of the virtual router.
<code>master</code>	Sets the default state of the VRRP router within the Virtual Router as <code>master</code> . For <code>master</code> , the router must own the Virtual IP address.
<code>backup</code>	Sets the default state of the VRRP router within the Virtual Router as <code>backup</code> .

Mode Router mode

Example

```
awplus#configure terminal
awplus(config)#router vrrp 5 vlan2
awplus(config-router)#virtual-ip 10.10.20.30 master
```

vrrp vmac

Use this command to enable or disable the Virtual MAC feature.

Syntax `vrrp vmac {enable|disable}`

Mode Global Configuration mode

Example To enable Virtual MAC enter:

```
awplus#configure terminal
awplus(config)#vrrp vmac enable
```

To disable Virtual MAC enter:

```
awplus#configure terminal
awplus(config)#vrrp vmac disable
```