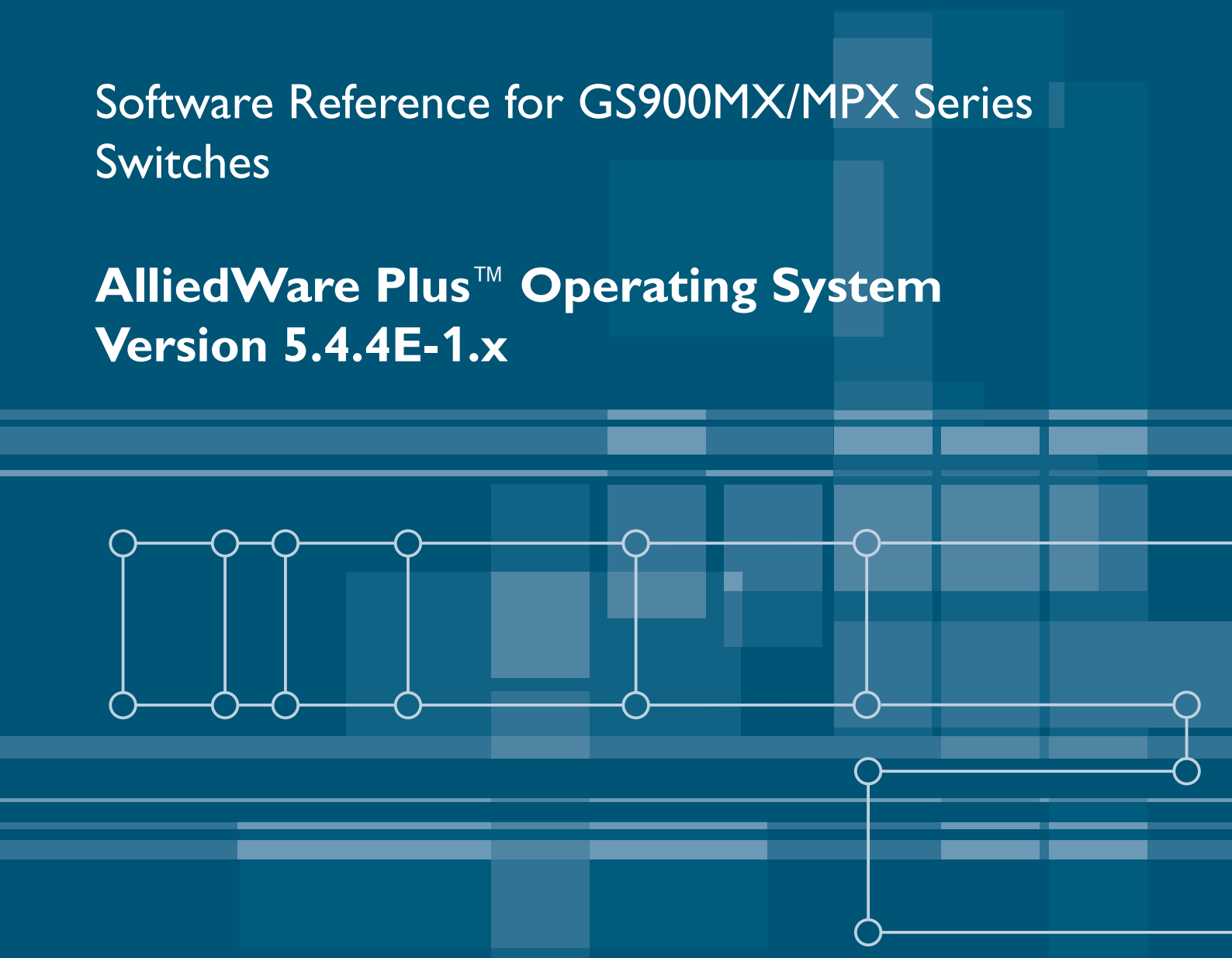
Software Reference for GS900MX/MPX Series Switches

AlliedWare Plus™ Operating System Version 5.4.4E-1.x



AT-GS924MX
AT-GS924MPX
AT-GS948MX
AT-GS948MPX

C613-50065-01 REV B

Allied Telesis

Acknowledgments

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

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

All rights reserved.

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

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

This product includes software licensed under the GNU General Public License available from: **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 Center at: **www.alliedtelesis.com/support/default.aspx**

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

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

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

©2015 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, AlliedWare Plus, EPSRing, SwitchBlade, and VCStack are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Getting the most from this manual

Although you can view this document using Acrobat version 5, to get the best from this manual, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

Table of Contents

Part 1: Setting up the Switch

Chapter 1: Getting Started

Introduction 1.2
How to Login 1.2
How to Get Command Help 1.3
Viewing a List of Valid Parameters 1.3
Completing Keywords 1.5
Viewing Command Error Messages 1.6
How to Work with Command Modes 1.7
Entering Privileged Exec Commands when in a Configuration Mode 1.9
How to See the Current Configuration 1.10
Default Settings 1.11
The Default Configuration 1.12
How to Change the Password 1.13
How to Set Strong Passwords 1.14
How to Set an IP Address on VLAN 1 ..... 1.16
How to Save and Boot from the Current Configuration 1.17
How to Save to the Default Configuration File 1.17
How to Create and Use a New Configuration File 1.17
How to Return to the Factory Defaults 1.19
How to See System Information 1.20
Viewing Overall System Information 1.20
Viewing Voltage, Fan Status, and Temperature 1.20
Viewing the Serial Number 1.21
How to Set System Parameters 1.22
How to Change the Telnet Session Timeout 1.22
How to Name the Switch 1.23
How to Display a Text Banner at Login 1.24
How to Set the Time and Date 1.25
How to Show Current Settings 1.25
How to Set the Time and Date 1.25
How to Set the Timezone 1.26
How to Configure Summer-Time 1.26
How to Add and Remove Users 1.27
Pre-Encrypted Passwords 1.28
How to Undo Settings 1.30
How to Use the *no* Parameter 1.30
How to Use the *default* Parameter 1.30
How to Upgrade the Firmware 1.31
Save Power with the Eco-Friendly Feature 1.32
The Eco-Friendly LED Feature 1.32
The Eco-Friendly LPI Feature 1.32
Trouble-shoot Fiber and Pluggable Issues 1.33
Using the Find Me feature 1.34
Controlling “show” Command Output 1.35

Chapter 2: Command Syntax Conventions in this Software Reference

Chapter 3: Start-Up Sequence

AlliedWare Plus Start-Up 3.2
Diagnostic Menu 3.3
Bootloader Menu 3.4
Start-Up Sequence 3.10

Chapter 4: CLI Navigation Commands

Command List 4.2

Chapter 5: User Access Commands

Introduction 5.2
Command List 5.2
- Using plain passwords 5.5
- Using encrypted passwords 5.5
- Using hidden passwords 5.6
- Using plain passwords 5.8
- Using encrypted passwords 5.8
- Using hidden passwords 5.9

Chapter 6: Creating and Managing Files

Introduction 6.2
USB Support 6.2
Working with Files 6.2
- Listing Files 6.3
- Displaying the Contents of Configuration and Text Files 6.4
- Navigating Through the File System 6.4
- Using the Editor 6.6

Creating and Using Configuration Files 6.8
- Creating a Configuration File 6.8
- Specifying the Start-Up Configuration Script 6.8
- Working with Configuration Files 6.9
- The Configuration File Fallback Order 6.10

Copying Files to and from Your Device 6.12
- URL Syntax 6.12
- Copying Files 6.13
- Copying from a Server to Running Configuration 6.17

The Autoboot Feature 6.19
- Restoring a Switch Using Autoboot from External Media 6.20
- Configure Autoboot 6.22

Chapter 7: File Management Commands

Introduction 7.3
- URL Syntax and Keyword Usage 7.3

Command List 7.5

Chapter 8: System Configuration and Monitoring Commands

Command List 8.2

Chapter 9: Debugging and Logging

Introduction 9.2
Debugging 9.2
Logging to a Terminal 9.2
Turning Off Debugging 9.3
Logging 9.3
Log Outputs 9.4

Chapter 10: Logging Commands

Command List 10.2

Chapter 11: Scripting Commands

Command List 11.2

Chapter 12: Interface Commands

Command List 12.2

Chapter 13: Interface Testing Commands

Command List 13.2

Part 2: Layer Two Switching

Chapter 14: Switching Introduction

Introduction 14.2
Physical Layer Information 14.3
Switch Ports 14.3
Activating and Deactivating Switch Ports 14.4
Autonegotiation 14.4
Duplex Mode 14.4
Speed Options 14.4
MDI/MDIX Connection Modes 14.5
The Layer 2 Switching Process 14.7
The Ingress Rules 14.7
The Learning Process 14.8
The Forwarding Process 14.9
The Egress Rules 14.9
Layer 2 Filtering 14.11
Ingress Filtering 14.11
Storm Control 14.12
Loop Protection 14.13
Loop Detection 14.13
Thrash Limiting 14.14
Support for Jumbo Frames 14.16
Port Mirroring 14.17
Port Security 14.18
IEEE 802.1X 14.18
Static MAC Address 14.18
Quality of Service 14.19
IGMP Snooping 14.20

Chapter 15: Switching Commands

Command List 15.2

Chapter 16: VLAN Introduction

VLANs Introduction 16.2
Virtual LANs (VLANs) 16.2
Configuring VLANs 16.3
Private VLANs 16.5
Private VLANs for Ports in Access Mode 16.5
Private VLAN Operation with Ports in Access Mode 16.7
Access Mode Private VLAN Configuration Example 16.8
Private VLANs for Trunked Ports 16.11
Trunked Port Private VLAN Configuration Example 16.12
Protocol Based VLAN Configuration Example 16.16

Chapter 17: VLAN Commands

Command List 17.2

Chapter 18: Spanning Tree Introduction: STP, RSTP, and MSTP

Introduction 18.2
Overview of Spanning Trees 18.2
Spanning Tree Operation 18.2
Spanning Tree Modes 18.4
Spanning Tree Protocol (STP) 18.5
Configuring STP 18.6
Rapid Spanning Tree Protocol (RSTP) 18.8
Configuring RSTP 18.9
Multiple Spanning Tree Protocol (MSTP) 18.11
Multiple Spanning Tree Instances (MSTI) 18.12
MSTP Regions 18.13
Common and Internal Spanning Tree (CIST) 18.15
MSTP Bridge Protocol Data Units (BPDUs) 18.17
Configuring MSTP 18.19

Chapter 19: Spanning Tree Commands

Command List 19.3

Chapter 20: Link Aggregation Introduction and Configuration

Introduction and Overview 20.2
Static and Dynamic (LACP) Link Aggregation 20.3
Static Channel Groups 20.3
Dynamic (LACP) Channel Groups 20.3
Link Aggregation Control Protocol (LACP) 20.3
Configuring an LACP Channel Group 20.5
Minimal LACP Group Configuration 20.8
Configuring a Static Channel Group 20.9

Chapter 21: Link Aggregation Commands

Introduction 21.2
Command List 21.3

Chapter 22: Power over Ethernet Introduction

Introduction 22.2
PoE Standards 22.2
PoE (all standards) 22.3
PoE (IEEE 802.3af) 22.3
Enhanced PoE 22.3
PoE+ (IEEE 802.3at) 22.3
Differences Between PoE and PoE+ 22.5
LLDP-MED (TIA-1057) with PoE+ (IEEE 802.3at) 22.5
PoE and PoE+ Applications 22.5
Power Device (PD) Discovery 22.5
Power Classes 22.6
Power through the Cable 22.7
Cable Types 22.8
Static and Automatic Power Allocation 22.8
PoE and PoE+ Implementation 22.9
Power Capacity 22.9
PoE Port Allocation and Distribution 22.9
Power Threshold 22.9
Negotiating Power Requirements 22.10
PoE Port Management 22.10
Powered Device (PD) Detection 22.10
Port Prioritization 22.10
Software Monitoring 22.12
PoE and PoE+ Configuration 22.13
Add a Description for a PoE or PoE+ Port 22.13
Configuring Capacity and Priority on a PoE or PoE+ Port 22.14
Remotely Monitoring Power for all Connected PDs 22.15

Chapter 23: Power over Ethernet Commands

Introduction 23.2
Command List 23.2

Part 3: IP and IPv6

Chapter 24: Internet Protocol (IP) Addressing and Protocols

Introduction 24.2
Address Resolution Protocol (ARP) 24.3
Static ARP Entries 24.3
Timing Out ARP Entries 24.3
Deleting ARP Entries 24.4
ARP Logging 24.5
DNS Client 24.6
Internet Control Message Protocol (ICMP) 24.8
Checking IP Connections 24.9
Ping 24.9
Traceroute 24.9

Chapter 25: IP Addressing and Protocol Commands

Introduction 25.2
Command List 25.3

Chapter 26: IPv6 Introduction

Introduction 26.2
Overview 26.2
IPv6 Addresses and Prefixes 26.3
Address Types 26.3
IPv6 Headers 26.4
The Internet Control Message Protocol (ICMPv6) 26.7
IPv6 Routing 26.10
Integration of IPv4 and IPv6 ..... 26.10
IPv6 on your Switch 26.11
Enabling IPv6 ..... 26.11
IPv6 Stateless Address Autoconfiguration (SLAAC) 26.11
IPv6 EUI-64 Addressing 26.11
IPv6 Link-local Addresses 26.12

Chapter 27: IPv6 Commands

Command List 27.2

Chapter 28: Route Selection

Introduction 28.2
Types of Routes 28.2
Interface Routes 28.2
Static Routes 28.2
RIP Routes 28.3
RIB and FIB Routing Tables 28.4
Understanding the Routing Information Base (RIB) 28.4
Administrative Distance 28.5
Metric 28.6
Equal Cost Multipath Routing 28.7
How AlliedWare Plus Deletes Routes 28.7
How AlliedWare Plus Adds Routes 28.8
Troubleshooting Routes not Installed in the RIB 28.9
Troubleshooting Routes not Installed in the FIB 28.9

Chapter 29: Routing Commands

Introduction 29.2
Command List 29.3

Chapter 30: RIP Configuration

Introduction 30.2
Enabling RIP 30.2
Specifying the RIP Version 30.4
RIPv2 Authentication (Single Key) 30.6
RIPv2 Text Authentication (Multiple Keys) 30.8
RIPv2 md5 authentication (Multiple Keys) 30.12

Chapter 31: RIP Commands

Introduction 31.2
Command List 31.3

Part 4: Multicast Applications

Chapter 32: IGMP Snooping Introduction

Introduction 32.2
IGMP 32.3
Joining a Multicast Group (Membership Report) 32.4
Staying in the Multicast Group (Query Message) 32.4
Leaving the Multicast Group (Leave Message) 32.4
IGMP Snooping 32.5
How IGMP Snooping Operates 32.5
IGMP Snooping and Querier Configuration Example 32.6
Query Solicitation 32.9
How Query Solicitation Works 32.9
Query Solicitation Operation 32.9
Speeding up IGMP Convergence in a Non-Looped Topology 32.12
Enabling Query Solicitation on Multiple Switches in a Looped Topology 32.12

Chapter 33: IGMP Snooping Commands

Introduction 33.2
Command List 33.2

Chapter 34: MLD Snooping Introduction and Configuration

Introduction 34.2
MLD Snooping 34.2

Chapter 35: MLD Snooping Commands

Command List 35.2

Part 5: Access and Security

Chapter 36: Access Control Lists Introduction

Introduction 36.2
Overview 36.2
ACL Rules 36.3
ACL Source and Destination Addresses 36.3
ACL Reverse Masking 36.3
Hardware and Software ACL Types 36.4
Defining Hardware MAC ACLs 36.5
Defining Hardware IP ACLs 36.6
Actions for Hardware ACLs 36.7
Attaching Hardware ACLs to Interfaces 36.7
Hardware ACLs and QoS Classifications 36.8
Classifying Your Traffic 36.8
Security ACLs 36.8
QoS ACLs 36.9
Attaching Hardware ACLs Using QoS 36.9
Filtering Hardware ACLs with QoS 36.11
Using QoS Match Commands with TCP Flags 36.11
ACL Filter Sequence Numbers 36.14
ACL Filter Sequence Number Behavior 36.14
ACL Filter Sequence Number Applicability 36.14

ACL Filter Sequence Number Types 36.15
ACL Filter Sequence Configuration 36.18
Creating ACLs in Global Configuration Mode 36.20
Display the ACL configuration details 36.22

Chapter 37: IPv4 Hardware Access Control List (ACL) Commands

Introduction 37.2
IPv4 Hardware Access List Commands and Prompts 37.3
Command List 37.4

Chapter 38: IPv4 Software Access Control List (ACL) Commands

Introduction 38.2
IPv4 Software Access List Commands and Prompts 38.3
Command List 38.4

Chapter 39: IPv6 Software Access Control List (ACL) Commands

Introduction 39.2
IPv6 Software Access List Commands and Prompts 39.3
Command List 39.4

Chapter 40: Quality of Service (QoS) Introduction

Introduction 40.2
QoS Operations 40.2
QoS Packet Information 40.3
Link Layer QoS 40.3
Differentiated Services Architecture 40.4
The Differential Services Field 40.5
Processing Pre-Marked Packets 40.6
Applying QoS on Your Switch 40.7
Classifying Your Data 40.7
Class Maps 40.7
Policy Maps 40.10
Premarking and Remarking Your Traffic 40.11
CoS to Egress Queue Premarking 40.11
DSCP to Egress Queue Premarking 40.13
Policing (Metering) Your Data 40.15
Single-Rate Three-Color Policing 40.15
Two-Rate Three-Color Policing 40.16
Configuring and Applying a Policer 40.17
Remarking Your Data 40.18
Configuring the Egress Queues 40.19
Egress Queues and QoS markers 40.19
Egress Queue Commands Hierarchy 40.19
Egress Queue Shaping 40.21
Scheduling 40.21
Drop Mode 40.22
Storm Protection 40.24

Chapter 41: QoS Commands

Command List 41.2

Chapter 42: Authentication Introduction and Configuration

Authentication Introduction 42.2
Configuring a Guest VLAN 42.2
802.1X-Authentication 42.3
Web-Authentication 42.4
What is Web-Authentication? 42.4
Web-Authentication Basics 42.4
Configuring Web-Authentication 42.6
Starting a Web-Authentication Session 42.8
Configuring an External Login Page 42.10
Customizing Web-Authentication Login Page 42.13
Support for Protocols Underlying Web-Authentication 42.15
Web-Authentication Timeout Connect 42.20
Web Authorization Proxy 42.21
MAC-Authentication 42.22
Why is MAC-Authentication Required? 42.22
How Does MAC-Authentication Work? 42.22
Configuring MAC-Authentication 42.23
Tri-Authentication 42.24
Tri-Authentication Configuration 42.25
Two-Step Authentication 42.27
Ensuring Authentication Methods Require Different Usernames and Passwords 42.28
Roaming Authentication 42.29
Roaming Authentication Overview 42.30
Roaming Authentication Feature Interactions 42.31
Unauthenticated Supplicant Traffic 42.32
Deciding When a Supplicant Fails Authentication 42.34
Failed Authentication VLAN 42.35
Limitations on Allowed Feature Combinations 42.35

Chapter 43: Authentication Commands

Command List 43.3

Chapter 44: AAA Introduction and Configuration

AAA Introduction 44.2
Available Functions and Server Types 44.2
Server Groups and Method Lists 44.3
Configuring AAA Login Authentication 44.5
AAA Configuration Tasks 44.5
Sample Authentication Configurations 44.7
Sample 802.1X-Authentication Configuration 44.7
Sample MAC-Authentication Configuration 44.8
Sample Web-Authentication Configuration 44.9
Sample Tri-Authentication Configuration 44.10

Chapter 45: AAA Commands

Command List 45.2

Chapter 46: 802.1X Introduction and Configuration

Introduction 46.2
802.1X System Components 46.2
The 802.1X Implementation 46.5
Configuring 802.1X 46.6

Chapter 47: 802.1X Commands

Command List 47.2

Chapter 48: RADIUS Introduction and Configuration

Introduction 48.2
RADIUS Packets 48.3
RADIUS Attributes 48.4
RADIUS Security 48.5
RADIUS Proxy 48.6
RADIUS Accounting 48.7
RADIUS Configuration 48.9
Switch Configuration Tasks 48.9
Switch to RADIUS Server Communication 48.10
AAA Server Groups Configuration 48.12
RADIUS Configuration Examples 48.15
RADIUS Authentication 48.15
Single RADIUS Server Configuration 48.16
Multiple RADIUS Server Configuration 48.17
RADIUS Server Group Configuration 48.17
RADIUS Server Configuration using Server Groups 48.18

Chapter 49: RADIUS Commands

Command List 49.2

Chapter 50: TACACS+ Introduction and Configuration

Introduction 50.2
TACACS+ Overview 50.2
The AlliedWare Plus TACACS+ Implementation 50.2
Authentication 50.3
Authorization 50.3
Accounting 50.4
Configuration 50.5
Configure TACACS+ 50.5
TACACS+ Configuration Example 50.7

Chapter 51: TACACS+ Commands

Command List 51.2

Chapter 52: Secure Shell (SSH) Introduction

Introduction 52.2
Secure Shell on the AlliedWare Plus OS 52.2
Configuring the SSH Server 52.4
Creating a Host Key 52.4
Enabling the Server 52.4
Modifying the Server 52.5
Validating the Server Configuration 52.6
Adding SSH Users 52.6
Authenticating SSH Users 52.7
Adding a Login Banner 52.7
Monitoring the Server and Managing Sessions 52.8
Debugging the Server 52.8
Configuring the SSH Client 52.9
Modifying the Client 52.9

Adding SSH Servers 52.10
Authenticating with a Server 52.10
Connecting to a Server and Running Commands 52.11
Copying files to and from the Server 52.11
Debugging the Client 52.11

Chapter 53: Secure Shell (SSH) Configuration

SSH Server Configuration Example 53.2

Chapter 54: Secure Shell (SSH) Commands

Introduction 54.2
Command List 54.2

Chapter 55: DHCP Snooping Introduction and Configuration

Introduction 55.2
DHCP Snooping 55.2
DHCP Snooping Database 55.3
DHCP Relay Agent Option 82 ..... 55.4
Traffic Filtering with DHCP Snooping 55.6
ARP Security 55.8
MAC Address Verification 55.8
DHCP Snooping Violations 55.8
Interactions with Other Features 55.9
Configuration 55.10
Configure DHCP Snooping 55.10
Disabling DHCP Snooping 55.16
Related Features 55.16

Chapter 56: DHCP Snooping Commands

Command List 56.2

Part 6: Network Availability

Chapter 57: EPSR Introduction and Configuration

Introduction 57.2
Ring Components and Operation 57.2
Fault Detection and Recovery 57.4
Fault Recovery 57.4
Restoring Normal Operation 57.5
Managing Rings with Two Breaks 57.6
Recovery When One Break is Restored 57.8
Configuration Examples 57.10
Single Domain, Single Ring Network 57.10
Single Ring, Dual Domain Network 57.16
Interconnected Rings 57.17
Superloop Protection 57.18
EPSR Superloop Prevention 57.19
Configuring a Basic Superloop Protected Two Ring EPSR Network 57.22
Sample Show Output 57.37
Adding a New Data VLAN to a Functioning Superloop Topology 57.41
EPSR and Spanning Tree Operation 57.44

Chapter 58: EPSR Commands

Command List 58.2

Chapter 59: RRP Snooping Introduction and Commands

RRP Snooping Introduction 59.2
Command List 59.3

Part 7: Network Management

Chapter 60: AMF Introduction and Configuration

Introduction to AMF 60.2
AMF on GS900MX/MPX Series Switches: AMF Edge 60.2
AMF Supported Products and Software Versions 60.2
Key Benefits of AMF 60.4
- Unified Command-Line 60.4
- Configuration Backup and Recovery 60.4
- Rolling-Reboot Upgrade 60.4
- Node Provisioning 60.5

AMF Terminology and Introduction 60.6
- AMF Network 60.6
- AMF Nodes 60.6
- Node Licensing 60.6
- Node Interconnection 60.7
- AMF Domains 60.7

AMF Network Operational Concepts 60.9
- Retention and Use of the 'Manager' Username 60.9
- Working-Set 60.9
- AMF Restricted Login 60.10
- Loop-Free Data Plane 60.10
- Aggregators 60.10
- VCStacks 60.10
- AMF External Removable Media 60.10
- AMF Interaction with QoS and ACLs 60.11
- NTP and AMF 60.11

Configuring AMF 60.13
Verifying the AMF Network 60.19
Configuring Multiple Nodes at the Same Time: the Unified CLI 60.21
- Working-Set Groups 60.22
- Executing Commands on Working-Sets 60.23
- Interactive Commands 60.26

AMF Backups 60.27
- Using External Media Storage 60.27
- Performing a Manual Backup 60.28
- Backing up to Remote Servers 60.29

Node Recovery 60.31
- Automatic Node Recovery 60.31
- Restoring a Node to a "Clean" State 60.32
- Manual Node Recovery 60.33
- Node Recovery on VCStacks 60.34

AMF Safe Configuration 60.35
- Detecting AMF Safe Configuration Operation 60.35
- AMF Safe Configuration Procedures 60.35
- Undoing an AMF Safe Configuration 60.36

Rolling-Reboot Firmware Upgrade 60.38
Performing a Rolling-Reboot Upgrade 60.40
Node Provisioning 60.42

Chapter 61: AMF Commands

Introduction 61.3
AMF on GS900MX/MPX Series Switches: AMF Edge 61.3
AMF Naming Convention 61.3

Chapter 62: NTP Introduction and Configuration

Introduction 62.2
Overview 62.2
NTP on the Switch 62.3
Troubleshooting 62.4
Configuration Example 62.5

Chapter 63: NTP Commands

Command List 63.2

Chapter 64: Dynamic Host Configuration Protocol (DHCP) Introduction

Introduction 64.2
DHCP 64.2
DHCP Relay Agents 64.2
Configuring the DHCP Client 64.3
DHCP Relay Agent Introduction 64.4
Configuring the DHCP Relay Agent 64.4
DHCP Relay Agent Information Option (Option 82) 64.5

Chapter 65: Dynamic Host Configuration Protocol (DHCP) Commands

Command List 65.2

Chapter 66: SNMP Introduction

Introduction 66.2
Network Management Framework 66.2
Structure of Management Information 66.4
Names 66.5
Instances 66.6
Syntax 66.7
Access 66.7
Status 66.7
Description 66.7
The SNMP Protocol 66.8
SNMP Versions 66.8
SNMP Messages 66.9
Polling versus Event Notification 66.9
Message Format for SNMPv1 and SNMPv2c 66.10
SNMP Communities (Version v1 and v2c) 66.11
SNMPv3 Entities 66.11
SNMPv3 Message Protocol Format 66.12
SNMPv1 and SNMPv2c 66.13
SNMP MIB Views for SNMPv1 and SNMPv2c 66.13
SNMP Communities 66.13

Configuration Example (SNMPv1 and v2) 66.15
SNMPv3 ..... 66.18
SNMP MIB Views for SNMPv3 ..... 66.18
SNMP Groups 66.18
SNMP Users 66.18
Configuration Example (SNMPv3) 66.19
Using SNMP to Manage Files and Software 66.20
Copy a File to or from a TFTP Server 66.20
Upgrade Software and Configuration Files 66.22

Chapter 67: SNMP Commands

Command List 67.2

Chapter 68: SNMP MIBs

Introduction 68.2
About MIBs 68.2
About SNMP 68.2
Obtaining MIBs 68.2
Loading MIBs 68.3
Allied Telesis Enterprise MIB 68.5
AT-ALMMON-MIB 68.6
AT-ATMF-MIB 68.8
AT-BOARDS-MIB 68.13
AT-DHCPSN-MIB 68.17
AT-DNS-CLIENT-MIB 68.20
AT-ENVMONv2-MIB 68.21
AT-EPSRv2-MIB 68.29
AT-FILEv2-MIB 68.32
AT-IP-MIB 68.39
AT-LICENSE-MIB 68.41
AT-LOG-MIB 68.44
AT-LOOPPROTECT-MIB 68.46
AT-MIBVERSION-MIB 68.48
AT-NTP-MIB 68.49
AT-PRODUCTS-MIB 68.52
AT-RESOURCE-MIB 68.55
AT-SETUP-MIB 68.57
AT-SMI-MIB 68.66
AT-SYSINFO-MIB 68.68
AT-TRIGGER-MIB 68.73
AT-USER-MIB 68.75
AT-VCSTACK-MIB 68.77
Other Enterprise MIBs 68.82
Public MIBs 68.83

Chapter 69: LLDP, LLDP-MED and Voice VLAN Introduction and Configuration

Introduction 69.2
Link Layer Discovery Protocol 69.2
LLDP-MED 69.3
Voice VLAN 69.3
LLDP Advertisements 69.4
Type-Length-Value (TLV) 69.4
LLDP-MED: Location Identification TLV 69.7
Transmission and Reception 69.8
LLDP-MED Operation 69.9

Storing LLDP Information 69.10
Configuring LLDP 69.11
Configure LLDP 69.12
Configure LLDP-MED 69.14
Configure Authentication for Voice VLAN 69.18

Chapter 70: LLDP Commands

Introduction 70.2
Command List 70.2

Chapter 71: SMTP Commands

Command List 71.2

Chapter 72: RMON Introduction and Configuration

Introduction 72.2
Overview 72.2
RMON Configuration Example 72.3

Chapter 73: RMON Commands

Command List 73.2

Chapter 74: Triggers Introduction

Introduction 74.2
Trigger Facility 74.2
Configuring a Trigger 74.2
Troubleshooting Triggers 74.5

Chapter 75: Triggers Configuration

Introduction 75.2
Restrict Internet Access 75.2
Capture Unusual CPU and RAM Activity 75.4
See Daily Statistics 75.6
Turn Off Power to Port LEDs 75.7
Reduce Power Supplied to Ports 75.9
Capture Show Output and Save to a USB Storage Device 75.11
Load a Release File From a USB Storage Device 75.12

Chapter 76: Trigger Commands

Command List 76.2

Chapter 77: Cable Fault Locator Introduction

Introduction to the Cable Fault Locator 77.2
Capabilities 77.2
TDR Operating Principles 77.2
Using the Cable Fault Locator 77.3

Chapter 78: Cable Fault Locator Commands

Command List 78.2

Chapter 79: Ping Polling Introduction and Configuration

Introduction 79.2
How Ping Polling Works 79.2
Configuring Ping Polling 79.4
Creating a Polling Instance 79.4
Customizing a Polling Instance 79.5
Troubleshooting Ping Polling 79.6
Interaction with Other Protocols 79.7

Chapter 80: Ping-Polling Commands

Command List 80.2

Part 8: Virtual Chassis Stacking

Chapter 81: VCStack Introduction

VCStack Introduction 81.2
Features of Virtual Chassis Stacking 81.2
VCStack Capable Switches 81.3
The Physical Stack 81.3
Two-Switch Stack Configuration 81.4
Multiple Switch Stack Configuration 81.4
Resilient Stacked Topology 81.5
Stack Formation 81.9
The Role of the Stack Master 81.9
Stack Management VLAN 81.10
Stack Member Failure and Recovery 81.13
Fixed or Virtual MAC Addressing 81.13
Stack Resiliency Link 81.14
Stack Failure Recovery 81.15
Stack Separation and Recovery 81.16
Stack Maintenance 81.16
Disabled Master Monitoring (DMM) 81.18
Provisioning (Stack Members) 81.20
Provisioned Board Classes 81.20
Applying Hardware Provisioning 81.20
Removing Hardware Provisioning 81.22
Displaying Provisioned Configurations 81.23
Provisioning and Configuration Management 81.24
Software Version Auto Synchronization 81.25
Introduction 81.25
How Auto Synchronization Works 81.25

Chapter 82: Stacking Commands

Introduction 82.2
Command List 82.3

Command List

Glossary

Part 1: Setting up the Switch

- Chapter 1 Getting Started
- Chapter 2 Command Syntax Conventions in this Software Reference
- Chapter 3 Start-Up Sequence
- Chapter 4 CLI Navigation Commands
- Chapter 5 User Access Commands
- Chapter 6 Creating and Managing Files
- Chapter 7 File Management Commands
- Chapter 8 System Configuration and Monitoring Commands
- Chapter 9 Debugging and Logging
- Chapter 10 Logging Commands
- Chapter 11 Scripting Commands
- Chapter 12 Interface Commands
- Chapter 13 Interface Testing Commands

Chapter 1: Getting Started

Introduction 1.2
How to Login 1.2
How to Get Command Help 1.3
Viewing a List of Valid Parameters 1.3
Completing Keywords 1.5
Viewing Command Error Messages 1.6
How to Work with Command Modes 1.7
Entering Privileged Exec Commands when in a Configuration Mode 1.9
How to See the Current Configuration 1.10
Default Settings 1.11
The Default Configuration 1.12
How to Change the Password 1.13
How to Set Strong Passwords 1.14
How to Set an IP Address on VLAN 1 ..... 1.16
How to Save and Boot from the Current Configuration 1.17
How to Save to the Default Configuration File 1.17
How to Create and Use a New Configuration File 1.17
How to Return to the Factory Defaults 1.19
How to See System Information 1.20
Viewing Overall System Information 1.20
Viewing Voltage, Fan Status, and Temperature 1.20
Viewing the Serial Number 1.21
How to Set System Parameters 1.22
How to Change the Telnet Session Timeout 1.22
How to Name the Switch 1.23
How to Display a Text Banner at Login 1.24
How to Set the Time and Date 1.25
How to Show Current Settings 1.25
How to Set the Time and Date 1.25
How to Set the Timezone 1.26
How to Configure Summer-Time 1.26
How to Add and Remove Users 1.27
Pre-Encrypted Passwords 1.28
How to Undo Settings 1.30
How to Use the *no* Parameter 1.30
How to Use the *default* Parameter 1.30
How to Upgrade the Firmware 1.31
Save Power with the Eco-Friendly Feature 1.32
The Eco-Friendly LED Feature 1.32
The Eco-Friendly LPI Feature 1.32
Trouble-shoot Fiber and Pluggable Issues 1.33
Using the Find Me feature 1.34
Controlling “show” Command Output 1.35

Introduction

This chapter introduces a number of commonly-used management features of the AlliedWare Plus™ Operating System (OS).

How to Login

Step 1: Set the console baud rate if necessary

The default baud rate is 9600.

By default the AlliedWare Plus™ OS supports VT100 compatible terminals on the console port. This means that the terminal size is 80 columns by 24 rows.

Step 2: Login with manager/friend

The defaults are:

```
username: manager
password: friend
```

The switch logs you into User Exec mode. From User Exec mode, you can perform high-level diagnostics (some **show** commands, ping, traceroute, for example), start sessions (Telnet, SSH), and change mode.

How to Get Command Help

The following kinds of command help are available:

- lists of valid parameters with brief descriptions (the ? key)
- completion of keywords (the Tab key)
- error messages for incomplete or incorrect syntax

Command Abbreviations

The AlliedWare Plus™ CLI contains a number of abbreviations for its commands. For example, the **show interface** command can be entered in the abbreviated form shown below:

```
awplus# sh in vlan100
```

Viewing a List of Valid Parameters

To get syntax help, type ? (i.e. “space question mark”) after:

- the prompt. This will list all commands available in the mode you are in.
- one or more parameters. This will list parameters that can come next in the partial command.
- one or more letters of a parameter. This will list matching parameters.

Note

The AlliedWare Plus™ OS only displays one screenful of text at a time, with the prompt “--More--” at the end of each screenful. Press the space bar to display the next screenful or the Q key to return to the command prompt.

Example

To see which commands are available in Privileged Exec mode, enter “?” at the Privileged Exec mode command prompt:

```
awplus# ?
```

This results in output as shown in **Figure 1-1** below:

Figure 1-1: Example output from the ? command

```
Exec commands:
activate         Activate a script
cd               Change the current working directory
clear            Reset functions
clock            Manage clock
configure        Enter configuration mode
copy             Copy from one file to another
.
.
.
```

Example

To see which **show** commands that start with “i” are available in Privileged Exec mode, enter “?” after **show i**:

```
awplus# show i?
```

This results in the following output:

Figure 1-2: Example output from the show i? command

```
interface          Select an interface to configure
ip                 Internet Protocol (IP)
ipv6               Internet Protocol version 6 (IPv6)
```

Examples To use the ? help to work out the syntax for the **clock timezone** command, enter the following sequence of commands:

```
awplus(config)# clock ?
```

```
summer-time  Manage summer-time
timezone     Set clock timezone
```

```
awplus(config)# clock timezone ?
```

```
TIMEZONE  Timezone name, up to 5 characters
```

```
awplus(config)# clock timezone NZST ?
```

```
minus  negative offset
plus   positive offset
```

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

```
<0-12>  Time zone offset to UTC
```

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

The above example demonstrates that the ? help only indicates what you can type **next**. For commands that have a series of parameters, like **clock timezone**, the ? help does not make the number of parameters obvious.

Completing Keywords

To complete keywords, type the Tab key after part of the command.

If only one keyword matches the partial command, the AlliedWare Plus™ OS fills in that keyword. If multiple keywords match, it lists them.

Examples In this example we use Tab completion in successive steps to build the complete command **show ip dhcp snooping**. We have included "<Tab>" to show where to type the Tab key — this is not displayed on screen.

Figure 1-3: Example output after entering the command show ip <Tab>

```
dhcp                dhcp-relay          domain-list
domain-name         extcommunity-list   filter
forwarding          igmp                interface
irdp                mroute              mvif
name-server         nat
pim                 protocols           rip
route               rpf
```

Figure 1-4: Example output after entering the command, show ip d<Tab>

```
awplus#show ip d<Tab>
dhcp          dhcp-relay       domain-list      domain-name
```

Figure 1-5: Example output from the show ip dhcp <Tab> command

```
awplus#show ip dhcp <Tab>
binding   pool      server    snooping
```

Figure 1-6: Example output from the show ip dhcp s<Tab> command

```
awplus#show ip dhcp s<Tab>
server    snooping
```

Viewing Command Error Messages

The switch displays the following generic error messages about command input:

% Incomplete command—this message indicates that the command requires more parameters. Use the ? help to find out what other parameters are available.

```
awplus# interface
```

```
% Incomplete command.
```

% Invalid input detected at '^' marker—this indicates that the switch could not process the command you entered. The switch also prints the command and marks the first invalid character by putting a '^' under it. Note that you may get this error if you enter a command in the wrong mode, as the following output shows.

```
awplus# interface port1.0.1
```

```
interface port1.0.1
          ^
% Invalid input detected at '^' marker.
```

% Unrecognized command—when you try to use ? help and get this message, it indicates that the switch can not provide help on the command because it does not recognize it. This means the command does not exist, or that you have entered it in the wrong mode, as the following output shows.

```
awplus# interface ?
```

```
% Unrecognized command
```

Note

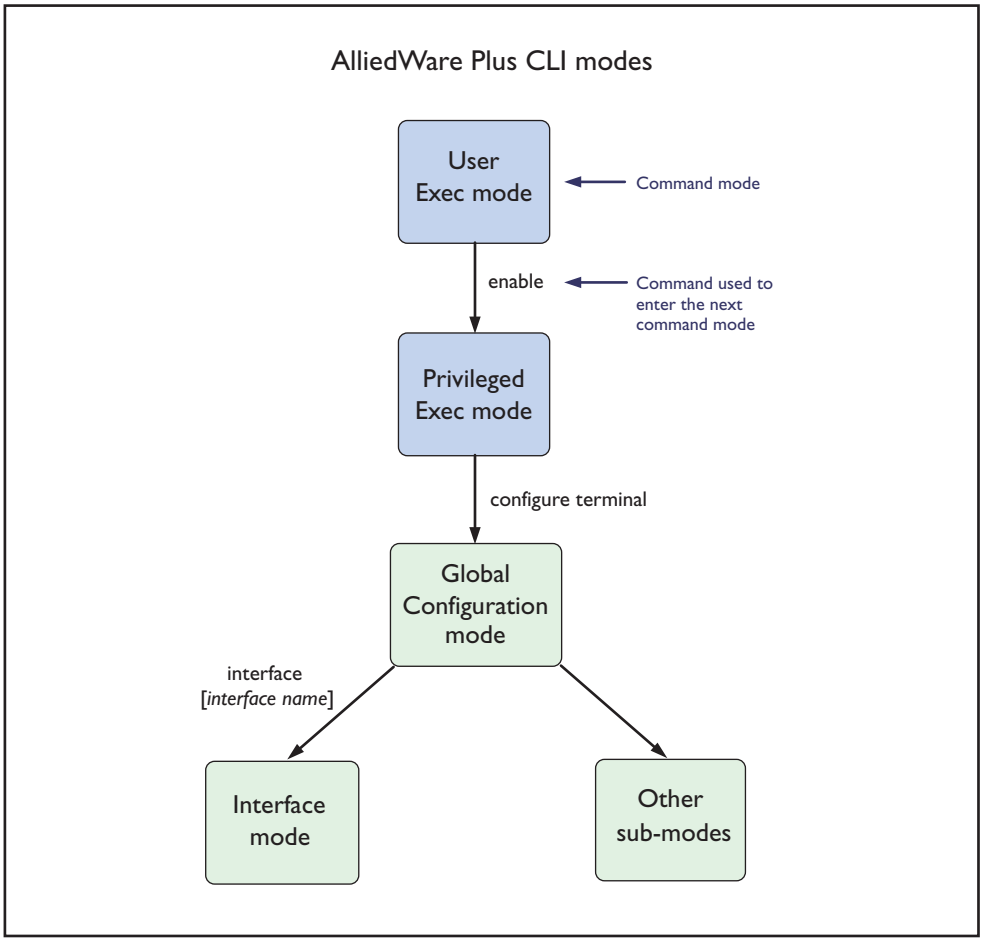
The AlliedWare Plus™ OS does not tell you when commands are successful. If it does not display an error message, you can assume the command was successful.

How to Work with Command Modes

The following figure shows the command mode hierarchy and the commands you use to move to lower-level modes.

Multiple users can telnet and issue commands using the User Exec mode and the Privileged Exec mode. However, only one user is allowed to use the Configure mode at a time. This prevents multiple users from issuing configuration commands simultaneously.

Figure 1-7: AlliedWare Plus™ CLI modes



User Exec mode

User Exec mode is the mode you log into on the switch.

It lets you perform high-level diagnostics (**show** commands, ping, traceroute, for example), start sessions (Telnet, SSH), and change mode.

The default User Exec mode prompt is **awplus>**

Privileged Exec mode

To change from User Exec to Privileged Exec mode, enter the command:

```
awplus# enable
```

Privileged Exec mode is the main mode for monitoring—for example, running **show** commands and debugging. From Privileged Exec mode, you can do all the commands from User Exec mode plus many system commands.

The default Privileged Exec mode prompt is **awplus#**

Global Configuration mode

To change from Privileged Exec to Global Configuration mode, enter the command:

```
awplus# configure terminal
```

From Global Configuration mode, you can configure most aspects of the switch.

The default Global Configuration mode prompt is **awplus(config)#**

Lower-level configuration modes

A number of features are configured by entering a lower-level mode from Global Configuration mode.

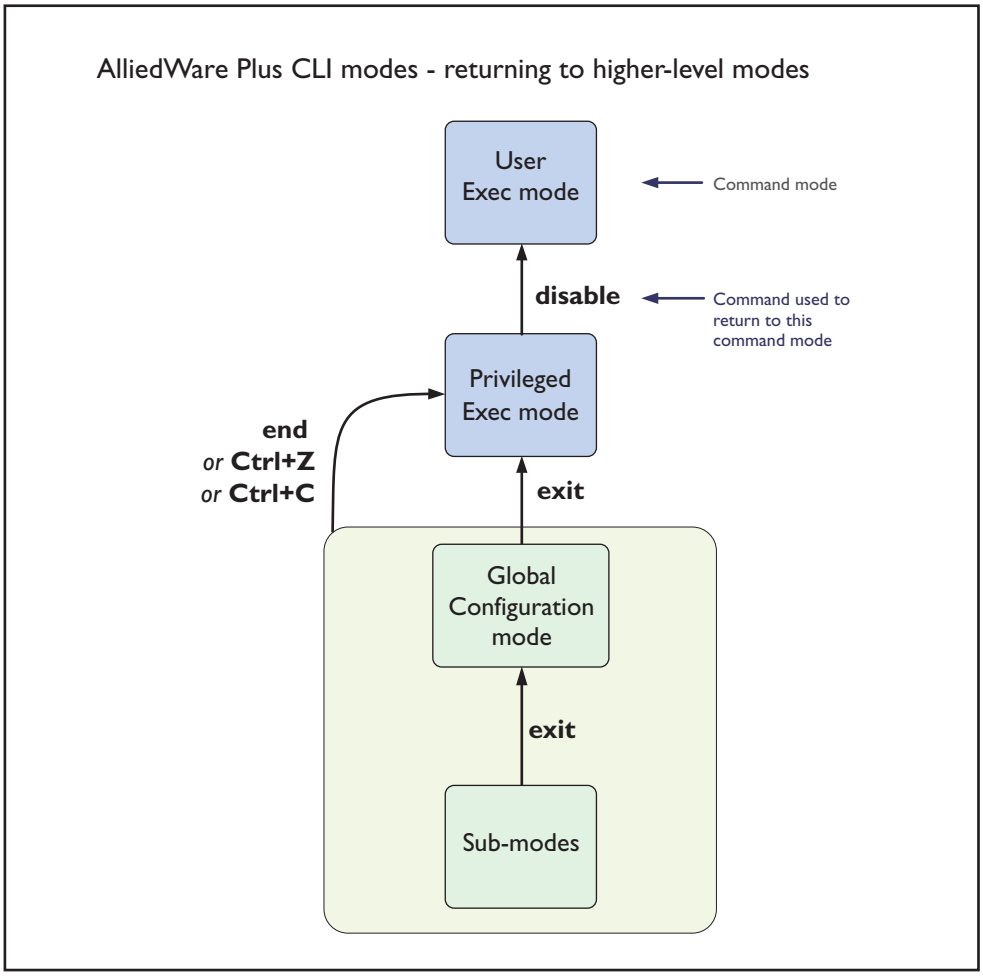
Some protocols have commands in both Global Configuration mode and lower-level configuration modes. For example, to configure MSTP, you use:

- Global Configuration mode to select MSTP as the spanning tree mode
- MST mode to create instances and specify other MSTP settings
- Interface Configuration mode to associate the instances with the appropriate ports.

Returning to higher-level modes

The following figure shows the commands to use to move from a lower-level mode to a higher-level mode.

Figure 1-8: Returning to higher-level modes



Examples To go from Interface Configuration to Global Configuration mode:

```
awplus(config-if)# exit
   awplus(config)#
```

To go from Interface Configuration to Privileged Exec mode:

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

To go from Privileged Exec to User Exec:

```
          awplus# exit
          awplus>
```

Entering Privileged Exec Commands when in a Configuration Mode

As you configure the switch you will be constantly entering various **show** commands to confirm your configuration. This requires constantly changing between configuration modes and Privileged Exec mode.

However, you can run Privileged Exec commands without changing mode, by using the command:

```
do <command you want to run>
```

You cannot use the ? help to find out command syntax when using the **do** command.

Example To display information about the IP interfaces when in Global Configuration mode, enter the command:

This results in the following output:

```
awplus(config)# do show ip int brief
```

Figure 1-9: Example output after entering the command "do show ip int brief"

```
Interface          IP-Address      Status          Protocol
vlan1              unassigned      admin up        running
vlan2              unassigned      admin up        running
```

How to See the Current Configuration

The current configuration is called the running-config. To see it, enter the following command in either Privileged Exec mode or any configuration mode:

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

To see only part of the current configuration, enter the command:

```
awplus# show running-config|include <word>
```

This displays only the lines that contain *word*.

To start the display at a particular place, enter the command:

```
awplus# show running-config|begin <word>
```

This searches the running-config for the first instance of *word* and begins the display from that line.

Note

The **show running-config** command works in all modes except User Exec mode.

Default Settings

When the switch first starts up with the AlliedWare Plus™ OS, it applies default settings and copies these defaults dynamically into its running-config.

These default settings mean that the AlliedWare Plus™ OS:

- encrypts passwords, such as user passwords
- records log message priority in log messages
- turns on the telnet server so that you can telnet to the switch
- enables the switch to look up domain names (but for domain name lookups to work, you have to configure a DNS server)
- turns off L3 multicast packet switching in the switch's hardware. This prevents L3 multicast from flooding the switch's CPU in its default state as an L2 switch
- sets the maximum number of ECMP routes to 4
- turns on RSTP on all ports. Note that the ports are not set to be edge ports
- sets all the switch ports to access mode. This means they are untagged ports, suitable for connecting to hosts
- creates VLAN 1and adds all the switch ports to it
- allows logins on the serial console port
- allows logins on VTY sessions (for telnet, for example)
- has switching enabled, so Layer 2 traffic is forwarded appropriately without further configuration
- allocates all the routing table memory space to IPv4 and IPv6 routes
- has ports set to autonegotiate their speed and duplex mode
- has copper ports set to auto MDI/MDI-X mode

The Default Configuration

Most of the above default settings are in the form of commands, which the switch copies to its running-config when it first boots up.

For more information about start-up files, see **"How to Save and Boot from the Current Configuration" on page 1.17**.

How to Change the Password

To change the password for the manager account, enter Global Configuration mode and enter the following command:

```
awplus(config)# username manager password <new-password>
```

The password can be up to 23 characters in length and include characters from up to four categories. The password categories are:

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

How to Set Strong Passwords

The password security rules are disabled by default. To set password security rules for users with administrative rights, or privilege level 15, enter Global Configuration mode.

You can then either specify whether the user is forced to change an expired password at the next login, or specify whether the user is not allowed to login with an expired password. You will need to specify a password lifetime greater than 0 before selecting either of these features. Note that the **security-password forced-change** and the **security-password reject-expired-pwd** commands cannot be enabled concurrently.

Password lifetime

Enter the following command to specify the password lifetime in days:

```
awplus(config)# security-password lifetime <0-1000>
```

Note that the value 0 will disable lifetime functionality and passwords will never expire. If lifetime functionality is disabled, the **security-password forced-change** command and the **security-password warning** command are also disabled.

Password forced change

To specify that a user is forced to change an expired password at the next login, enter the following command:

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

If the **security-password forced-change** command is enabled, users with expired passwords are forced to change to a password that must comply with the current password security rules at the next login.

Reject expired password

To specify that a user is not allowed to login with an expired password, enter the following command:

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

If the **security-password reject-expired-pwd** command is enabled, users with expired passwords are rejected at login. Users then have to contact the Network Administrator to change their password.

Caution

Once all users' passwords are expired you are unable to login to the device again if the security-password reject-expired-pwd command has been executed. You will have to reboot the device with a default configuration file, or load an earlier software version that does not have the security password feature.
We recommend you never have the command line "security-password reject-expired-pwd" in a default config file.

Use other password security rules to further configure password security settings.

Password warning

To specify the number of days before the password expires that the user will receive a warning message specifying the remaining lifetime of the password, enter the command:

```
awplus(config)# security-password warning <0-1000>
```

The value 0 will disable warning functionality and the warning period must be less than, or equal to, the password lifetime.

Password history

To specify the number of previous passwords that are unable to be reused enter the command:

```
awplus(config)# security-password history <0-15>
```

The value `0` will disable history functionality. If history functionality is disabled, all users' password history is reset and all password history is lost. A new password is invalid if it matches a password retained in the password history.

Password minimum length

To specify the minimum allowable password length, enter the command:

```
awplus(config)# security-password minimum-length <1-23>
```

Password minimum categories

To specify the minimum number of categories that the password must contain in order to be considered valid, enter the command:

```
awplus(config)# security-password minimum-categories <1-4>
```

The password categories are:

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

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

How to add a user is described in **"How to Add and Remove Users" on page 1.27**.

Display security password settings

To list the configuration settings for the various security password rules, enter the command:

```
awplus(config)# show security-password configuration
```

To list users remaining lifetime or last password change, enter the command:

```
awplus(config)# show security-password user
```

How to Set an IP Address on VLAN 1

This section describes how to set an IP address on the default VLAN (**vlan1**).

Step 1: If desired, check the current configuration

After logging in, enter Privileged Exec mode by using the command:

```
awplus# enable
```

Then check the current configuration by using one of the following commands:

```
awplus# show ip interface vlan1 brief
```

The output looks like this:

```
Interface            IP-Address      Status          Protocol
vlan1                172.28.8.200    admin up        running
```

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

This output looks like this:

```
!
interface vlan1
 ip address 172.28.8.200/16
!
```

Step 2: Enter Interface Configuration mode for the vlan1 interface

Enter Global Configuration mode and enter the command:

```
awplus(config)# interface vlan1
```

Step 3: Enter the IP address and mask

Enter the command:

```
awplus(config-if)# ip address <address/mask>
```

For example, to set the address to 172.28.8.210/16, enter the command:

```
awplus(config-if)# ip address 172.28.8.210/16
```

How to Save and Boot from the Current Configuration

This section tells you how to save your configuration and run the saved configuration when the switch starts up.

You can either:

- save the configuration to the switch's default configuration file (called "default.cfg"). By default, the switch uses that file at start-up.
- create a new configuration file and set the switch to use the new configuration file at start-up.

How to Save to the Default Configuration File

Enter Privileged Exec mode and enter the command:

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

The parameter **startup-config** is a short-cut for the current boot configuration file, which will be the default configuration file unless you have changed it, as described in the next section.

How to Create and Use a New Configuration File

Step 1: Copy the current configuration to a new file

Enter Privileged Exec mode and enter the command:

```
awplus# copy running-config <destination-url>
```

Example To save the current configuration in a file called `example.cfg`, enter the command

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

Step 2: Set the switch to use the new file at startup

To run the new file's configuration when the switch starts up, enter Global Configuration mode and enter the command:

```
awplus(config)# boot config-file <filepath-filename>
```

Note that you can set the switch to use a configuration file on a USB storage device if you have saved the configuration file to a USB storage device. You can only specify that the configuration file is on a USB storage device if there is a backup configuration file already specified in Flash.

To set a backup configuration file to load if the main configuration file cannot be loaded, enter the command:

```
awplus(config)# boot config-file backup <filepath-filename>
```

For an explanation of the configuration fallback order, see **"The Configuration File Fallback Order" on page 6.10**.

Example To run the commands in `example.cfg` on startup, enter the command:

```
awplus(config)# boot config-file flash:/example.cfg
```

To set `backup.cfg` as the backup to the main configuration file, enter the command:

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

Step 3: Display the new settings

To see the files that the switch uses at startup, enter Privileged Exec mode and enter the command:

```
awplus# show boot
```

The output looks like this:

```
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : flash:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/example.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file exists)
```

Step 4: Continue updating the file when you change the configuration

When you next want to save the current configuration, enter Privileged Exec mode and enter the command:

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

The parameter **startup-config** is a short-cut for the current boot configuration file.

How to Return to the Factory Defaults

The switch dynamically adds the default settings to the running-config at start-up if the default file is not present. This section describes how to use this feature to return to the factory defaults.

Note

After reboot the show running-config output will show the default factory settings for your switch once you have removed the default.cfg file. To recreate the default.cfg file enter copy running-config startup-config. When you enter copy running-config startup-config commands the default.cfg file is updated with the startup-config.

Completely restore defaults

To completely remove your configuration and return to the factory default configuration, delete or rename the default file and make sure no other file is set as the start-up configuration file.

To find the location of the default boot configuration file, enter Privileged Exec mode and enter the command:

```
awplus# show boot
```

To delete the default file when it is the current boot configuration file, enter Privileged Exec mode and enter either of the commands:

```
awplus# delete force <filename>
```

or:

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

Note that erasing startup-config deletes the current boot configuration file—it does not simply stop the file from being the boot file.

To make sure that no other file is loaded at start-up, enter Global Configuration mode and enter the command:

```
awplus(config)# no boot config-file
```

Partially restore defaults

To partially restore the default settings, make a configuration file that contains the settings you want to keep and set this as the start-up configuration file. On start-up, the switch will add the missing settings to the running-config.

How to See System Information

This section describes how to view the following system information:

- overview information
- details of temperature and voltage
- serial number

Viewing Overall System Information

To display an overview of the switch hardware, software, and system settings, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system
```

The output looks like this:

```
GS900#show system
Stack System Status                                  Thu May 29 02:02:30 2014

Stack member 1

Board       ID  Bay   Board Name                        Rev   Serial number
-------------------------------------------------------------------------
Base       392        GS948MX                           X1-0  A04939H131100021
-------------------------------------------------------------------------
RAM:  Total: 494848 kB Free: 399396 kB
Flash: 62.0MB Used: 45.4MB Available: 16.6MB
-------------------------------------------------------------------------
Environment Status : Normal
Uptime             : 0 days 00:02:30
Bootloader version : 3.0.3-devel


Current software   : GS900-5.4.4E-1.1.rel
Software version   : Version 5.4.4E-1
Build date         : Thu May 29 01:32:39 NZST 2014

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

System Name
 GS900
System Contact

System Location

GS900#
```

Viewing Voltage, Fan Status, and Temperature

The switch monitors the environmental status of the switch and its power supplies and fan. To display this information, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system environment
```

The output looks like this:

```
GS900#show system environment
Environment Monitoring Status

Overall Status: Normal

Resource ID: 1  Name: GS948MX
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Voltage: 1.8V (Volts)                 1.810      1.612      1.975     Ok
2   Voltage: 1.0V (Volts)                 1.011      0.891      1.090     Ok
3   Voltage: 3.3V (Volts)                 3.351      3.028      3.545     Ok
4   Voltage: 5.0V (Volts)                 5.079      4.477      5.498     Ok
5   Voltage: 1.2V (Volts)                 1.215      1.046      1.292     Ok
6   Temp: CPU (Degrees C)                    56        -11         75     Ok
7   Temp: System (Degrees C)                 57        -11         80     Ok
GS900#
```

Viewing the Serial Number

The switch's serial number is displayed in the output of the **show system** command on page 8.46, but for convenience, you can also display it by itself. To do this, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system serialnumber
```

The output looks like this:

```
P1FY7502C
```

How to Set System Parameters

You can set system parameters to personalize the switch and make it easy to identify it when troubleshooting. This section describes how to configure the following system parameters:

- telnet session timeout
- switch name
- login banner

How to Change the Telnet Session Timeout

By default, telnet sessions time out after 10 minutes of idle time. If desired, you can change this.

To change the timeout for all telnet sessions, enter Global Configuration mode and enter the commands:

```
awplus(config)# line vty 0 32
awplus(config-line)# exec-timeout <new-timeout>
```

The new timeout value only applies to new sessions, not current sessions.

Examples To set the timeout to 30 minutes, enter the command:

```
awplus(config-line)# exec-timeout 30
```

To set the timeout to 30 seconds, enter the command:

```
awplus(config-line)# exec-timeout 0 30
```

To set the timeout to infinity, so that sessions never time out, enter either of the commands:

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

How to Name the Switch

To give the switch a name, enter Global Configuration mode and enter the command:

```
awplus(config)# hostname <name>
```

For example, to name the switch “mycompany”:

```
awplus(config)# hostname mycompany
```

The prompt displays the new name:

```
mycompany(config)#
```

The name can contain hyphens and underscore characters, for example:

```
mycompany(config)#hostname mycompany_more_words
mycompany_more_words(config)#hostname mycompany-hyphenated
mycompany-hyphenated(config)
```

However, the name must be a single word, as the following example shows.

```
mycompany(config)#hostname mycompany more words
                                   ^
% Invalid input detected at '^' marker.
```

It also cannot be surrounded by quote marks, as the following example shows.

```
awplus(config)#hostname "mycompany more words"
% hostname contains invalid characters
```

Removing the name

To remove the hostname, enter the command:

```
mycompany(config)# no hostname
```

The prompt changes back to the default prompt:

```
awplus(config)#
```

How to Display a Text Banner at Login

By default, the switch displays the AlliedWare Plus™ OS version and build date before login. You can customize this by changing the Message of the Day (MOTD) banner.

To enter a new MOTD banner, enter Global Configuration mode and enter the command:

```
awplus(config)# banner motd <banner-text>
```

The text can contain spaces and other printable characters. You do not have to surround words with quote marks.

Example

To display "this is a new banner" when someone logs in, enter the command:

```
awplus(config)# banner motd this is a new banner
```

This results in the following output at login:

```
awplus login: manager
Password:
this is a new banner
awplus>
```

Removing the banner

To return to the default banner (AlliedWare Plus™ OS version and build date), enter the command:

```
awplus(config)# banner motd default
```

To remove the banner instead of replacing it, enter the command:

```
awplus(config)# no banner motd
```

How to Set the Time and Date

There are three aspects to setting the time and date:

- setting the current time and date (**"How to Set the Time and Date" on page 1.25**)
- setting the timezone (**"How to Set the Timezone" on page 1.26**)
- configuring the switch to automatically change the time when summer-time begins and ends (**"How to Configure Summer-Time" on page 1.26**)

Instead of manually setting the time, you can use NTP to automatically get the time from another device.

How to Show Current Settings

To display the current time, timezone and date, enter Privileged Exec mode and enter the command:

```
awplus# show clock
```

The output looks like this:

```
UTC Time:   Wed,  16 May 2013 16:08:14 +0000
Timezone: UTC
Timezone Offset: +00:00
Summer time zone: None
```

How to Set the Time and Date

To set the time and date, enter Privileged Exec mode and enter the **clock set** command:

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

:where:

- *hh* is two digits giving the hours in 24-hour format (e.g. **14**)
- *mm* is two digits giving the minutes
- *ss* is two digits giving the seconds
- *day* is two digits giving the day of the month
- *month* is the first three letters of the month name (e.g. **sep**)
- *year* is four digits giving the year

Example To set the time to 14:00:00 on 25 January 2012, use the command:

```
awplus# clock set 14:00:00 25 jan 2012
```

How to Set the Timezone

To set the timezone, enter Global Configuration mode and enter the **clock timezone** command:

```
clock timezone <timezone-name> {plus|minus} <0-12>
```

The <*timezone-name*> can be any string up to 6 characters long.

To return the timezone to UTC+0, enter the command:

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

Example To set the timezone to Eastern Standard Time, use the command:

```
awplus(config)# clock timezone EST minus 5
```

How to Configure Summer-Time

There are two approaches for setting summer-time:

- *recurring*, when you specify the week when summer-time starts and ends and each year the switch changes the time at those weeks. For example, Eastern Daylight Time (EDT) starts at 2 am on the second Sunday in March and ends at 2 am on the first Sunday in November.
- *date-based*, when you specify the start and end dates for summer-time for a particular year. For example, Eastern Daylight Time (EDT) starts at 2 am on Sunday, 8 March 2008 and ends at 2 am on Sunday, 2 November 2008.

Recurring To set summer-time with recurring dates, enter Global Configuration mode and enter the **clock summer-time recurring** command:

```
clock summer-time <zone-name> recurring <start-week> <start-
day> <start-month> <start-time> <end-week> <end-day>
<end-month> <end-time> <1-180>
```

The <*zone-name*> can be any string up to 6 characters long.

The <*start-time*> and <*end-time*> are in the form `hh:mm`, in 24-hour time.

Note that if you specify 5 for the week, this changes the time on the last day of the month, not the 5th week.

Example To configure EDT, enter the command:

```
awplus(config)# clock summer-time EDT recurring 2 Sun Mar
                02:00 1 Sun Nov 02:00 60
```

Date-based To set summer-time for a single year, enter Global Configuration mode and enter the **clock summer-time date** command:

```
clock summer-time <zone-name> date <start-day> <start-month>
<start-year> <start-time> <end-day> <end-month> <end-year>
<end-time> <1-180>
```

The <*zone-name*> can be any string up to 6 characters long.

The <*start-time*> and <*end-time*> are in the form `hh:mm`, in 24-hour time.

Example For example, to configure EDT for 2008 enter the command:

```
awplus(config)# clock summer-time EDT date 8 Mar 2008 02:00
                2 Nov 2008 02:00 60
```

How to Add and Remove Users

Adding users To add a new user with administrative rights, enter Global Configuration mode and enter the command:

```
awplus(config)# username <name> privilege 15 password
                <password>
```

Both <*name*> and <*password*> can contain any printable character and are case sensitive.

When you add a user with administrative rights, <*password*> will have to conform to the following rules:

- **security-password minimum-categories** command on page 5.20
- **security-password minimum-length** command on page 5.21
- **security-password history** command on page 5.17. If this command is enabled, <*password*> is invalid if it matches a password retained in the password history.

The AlliedWare Plus™ OS gives you a choice of **1** or **15** for the privilege level. Level **1** users are limited to User Exec mode so you need to set most users to level **15**.

For example, to add user Bob with password 123$%^, enter the command:

```
awplus(config)# username Bob privilege 15 password 123$%^
```

Removing users To remove a user, enter Global Configuration mode and enter the command:

```
no username <name>
```

For example, to remove user Bob, enter the command:

```
awplus(config)# no username Bob
```

Note that you can delete all users, including the user called “manager” and the user you are logged in as. If all privilege **15** user accounts are deleted, a warning message is generated:

```
% Warning: No privileged users exist.
```

If all privilege level **15** user accounts are deleted, and there are no other users configured for the device, you may have to reboot with the default configuration file.

If there is a user account on the device with a lower privilege level and a password has already been set with the **enable password** command on page 5.4, you can login and still enter privileged mode. When executing the **enable** command, enter the password created with the **enable password** command. For example, if the password is mypassword:

```
awplus> enable mypassword
awplus#
```

Displaying users

To list the currently logged-in users, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show users
```

The output looks like this:

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

To list all configured users, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show running-config|include username
```

The output looks like this:

```
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
username Bob privilege 15 password 8 $1$gXJLY8dw$iqkMXLgQxbzSOutNUa5E2.
```

Pre-Encrypted Passwords

The running-config output above includes the number 8 after the **password** parameter. This indicates that the password is displayed in its encrypted form.

You can enter the number 8 and a pre-encrypted password on the command line. You may want to pre-encrypt passwords if you need to load them onto switches via an insecure method (such as HTTP, or by emailing them to remote users).

Caution Only enter the number 8 if you are entering a pre-encrypted password—otherwise, you will be unable to log in using the password and will be unable to access the switch through that username. The next section describes why.

Testing this feature

If you want to test the effect of this, *create a new user* for the test instead of using the manager user. The test stops you from logging in as the test user, so you need to have the manager user available to log in as.

The following output shows how specifying the number 8 puts the password into the running-config exactly as you typed it:

```
awplus(config)#username Bob privilege 15 password 8 friend
awplus(config)#show running-config |include username Bob
username Bob privilege 15 password 8 friend
```

After entering the command above, logging in as “Bob” with a password of “friend” does not work. This is because the switch takes the password you enter (“friend”), hashes it, and compares the hash with the string in the running-config (“friend”). The hashed value and “friend” are not the same, so the switch rejects the login.

How to Undo Settings

There are two possibilities for undoing settings: the **no** parameter and the **default** parameter.

How to Use the *no* Parameter

To undo most settings, simply re-enter the first parameters of the configuration command with the parameter **no** before them.

Example You can set the timezone to Eastern Standard Time by entering the command:

```
awplus(config)# clock timezone EST minus 5
```

To remove the timezone setting, enter the command:

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

How to Use the *default* Parameter

Some commands have a **default** parameter that returns the feature to its default setting.

Example You can change the login banner to “this is a new banner” by entering the command:

```
awplus(config)# banner motd this is a new banner
```

To return to the default banner, enter the command:

```
awplus(config)# banner motd default
```

Note that this command also has a **no** parameter that lets you remove the banner altogether.

How to Upgrade the Firmware

New releases of the AlliedWare Plus™ OS become available regularly. Contact your customer support representative for more information.

Step 1: Put the new release onto your TFTP server or your USB drive

Step 2: If necessary, create space in the switch's Flash memory for the new release

Note that you cannot delete the current release file.

To see how much space is free, use the command:

```
awplus# show file systems
```

Step 3: Copy the new release from your TFTP server or your USB drive onto the switch

Follow the relevant instructions in "Copying with Trivial File Transfer Protocol (TFTP)" on page 6.16, or "Copying to and from NVS or a USB storage device" on page 6.15.

Step 4: Set the switch to boot from the new release

Enter Global Configuration mode and enter the command:

```
awplus(config)# boot system <filepath-filename>
```

You can set a backup release file to load if the main release file cannot be loaded. Enter the command:

```
awplus(config)# boot system backup <filepath-filename>
```

Step 5: Check the boot settings

Enter Privileged Exec mode and enter the command:

```
awplus# show boot
```

Step 6: Reboot

Enter Privileged Exec mode and enter the command:

```
awplus# reboot
```

Save Power with the Eco-Friendly Feature

The Eco-Friendly LED Feature

You can conserve power by enabling the eco-friendly LED (Light Emitting Diode) feature either by entering the **ecofriendly led** command on page 8.12 or by pressing the **eco**-friendly button on the front panel. This feature disables power to the port LEDs, but not the power indicator LED. In the eco-friendly mode, one of the horizontal segments of the seven segment display will glow permanently. If the device is a stack master, the upper segment will glow; if the device is a stack member or a stand alone unit, the center segment will glow.

When the eco-friendly LED feature is enabled, a port's LED will not change if the port's status changes. When the eco-friendly feature is disabled and power is returned to port LEDs, the LEDs will correctly show the current state of the ports.

In a stack environment, enabling the eco-friendly LED feature on the stack master will apply the feature to every member of the stack.

The eco-friendly LED feature is disabled by default. To globally enable the feature for all LED ports on the switch, either push the eco-switch button or enter the commands:

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

For an example of how to configure a trigger to enable the eco-friendly LED feature, see **"Turn Off Power to Port LEDs" on page 75.7**.

The Eco-Friendly LPI Feature

You can also conserve power by enabling the eco-friendly LPI (Low Power Idle) feature with the **ecofriendly lpi** command on page 8.13. This feature reduces the power supplied to the ports by the switch whenever the ports are idle and are connected to IEEE 802.3az Energy Efficient Ethernet compliant host devices. All ports configured for LPI must support LPI in hardware and must be configured to autonegotiate by default or by using the **speed** and **duplex** commands as needed.

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

The eco-friendly LPI (Low Power Idle) feature is disabled by default. To enable the feature for a switch port, or for a range of switch ports in the example below, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.6
awplus(config-if)# ecofriendly lpi
```

For an example of how to configure a trigger to enable the eco-friendly LPI feature, see **"Reduce Power Supplied to Ports" on page 75.9**.

Trouble-shoot Fiber and Pluggable Issues

Digital Diagnostics Monitoring (DDM) for SFP (1 Gigabit Small Form-factor Pluggable) and SFP+ (10 Gigabit Small Form-factor Pluggable) transceivers allows you to measure optical parameters for pluggables installed in a switch and trouble shoot fiber issues.

Fiber cable can be vulnerable to damage. Patch panels and patch cables can be connected with the wrong type of fiber, fiber splices can become faulty and fiber cables can be cut accidentally. Trouble shooting fiber issues has required special equipment and expertise to find the source of a problem causing signal attenuation. Digital monitoring features help find fiber issues.

Different types of transceivers are supported in different models of switch. See your Allied Telesis dealer for more information about the particular models of pluggables that your switch supports, and if these transceivers also support digital monitoring.

To display information about transceivers installed on your switch, enter the following command:

```
awplus# show system pluggable diagnostics
```

The following parameters are measured and are displayed in **show system pluggable diagnostics** command output:

- Temperature (Centigrade) inside the transceiver
- Vcc (Volts) voltage supplied to the transceiver
- Tx Bias (mA) current to the Laser Diode in the transceiver
- Tx Power (mW) the amount of light transmitted from the transceiver
- Rx Power (mW) the amount of light received in the transceiver

You can track Tx Bias to find out how the Laser Diode in the transceiver is aging by comparing the Tx Bias for one transceiver against Tx Bias for others. You can use this information to see if any transceivers may need replacement.

You can trouble shoot fiber connectivity issues by checking the Tx Power at one end of the fiber link against the Rx Power at the other end of the fiber link to measure the attenuation. Knowing the attenuation enables you to determine if there are anomalies in the fiber cable.

Note that Tx Power differences between the same type of transceivers installed on a switch may indicate that a transceiver is not seated or locked. Ensuring transceivers are seated and locked in place with the retaining clip will keep the fiber link up if there is any vibration or movement that can dislodge a fiber cable. Rx Power differences may indicate poor fiber patch cables, poor connectors or poor splices. Tracking Tx Bias for installed transceivers and measuring attenuation for fiber links allows you to perform periodic preventative maintenance, instead of reacting to a failure. Tracking Tx Power differences can be used as an indicator of failure in an which may need replacing.

Using the Find Me feature

The Find Me feature enables you to physically locate a specific device from a group of similar devices.

Running the **findme** command on page 8.15 causes the device's LEDs to alternately flash green and amber at a rate of 1 Hz. If the switch has no amber LED, then the green LED will flash on/off at a rate of 1 Hz.

An optional **interface** parameter specifies one or more interfaces to flash, while an optional **member** parameter specifies a particular stack member. Both these parameters are mutually exclusive. If no **interface** or **member** parameter is specified, then all ports on the device or stack are flashed.

An optional **timeout** parameter specifies the flash behavior **duration**. The default time is one minute (60 seconds). Normal LED behavior is restored automatically after either the default time, or a specified time, has elapsed or a **no findme** command is used.

Controlling “show” Command Output

You can control the output of **show** commands by using the | and > or >> tokens in the following ways:

- To display only part of the output, follow the command with **|** and then other keywords (see **Output modifiers** below)
- To save the output to a file, follow the command with **> filename**
- To append the output to an existing file, follow the command with >> **filename**

Using the ? after typing the **show** command displays the following information about these tokens:

```
awplus#  show users
```

```
| Output modifiers
> Output redirection
>> Output redirection (append)
```

Output modifiers

Type the | (vertical bar) to use **output modifiers**.

```
append    Append output
begin     Begin with the first line that contains
          matching output
exclude   Exclude lines that contain matching output
include   Include lines that contain matching output
redirect  Redirect output
```

Begin

The **begin** parameter causes the display to begin at the first line that contains the input string.

```
awplus#  show run | begin vlan1
```

```
...skipping
interface vlan1
 ip address 192.168.14.1
!!
line con 0
 login
line vty 0 4
 login
!
end
```

Exclude The **exclude** parameter excludes all lines of output that contain the input string. In the following output all lines containing the word "input" are excluded:

```
awplus#  show interface vlan1 | exclude input
```

```
Interface vlan1
  Scope: both
  Hardware is Ethernet, address is 192.168.14.1
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0,
window 0
    collisions 0
```

Include The include parameter includes only those lines of output that contain the input string. In the output below, all lines containing the word "input" are included:

```
awplus#  show interface vlan1 | include input
```

```
input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

Redirect The **redirect** parameter puts the lines of output into the specified file. If the file already exists, the new output overwrites the file's contents; the new output is not appended to the existing file contents.

| **redirect** and > are synonyms.

```
awplus#  show history | redirect history.txt
```

Output redirection The output redirection token > puts the lines of output into the specified file. If the file already exists, the new output overwrites the file's contents; the new output is not appended to the existing file contents.

| **redirect** and > are synonyms.

```
awplus#  show history > history.txt
```

Append output The append output token >> adds the lines of output into the specified file. The file must already exist, for the new output to be added to the end of the file's contents; the new output is appended to the existing file contents.

| **append** and >> are synonyms.

```
awplus#  show history >> history.txt
```

Chapter 2: Command Syntax Conventions in this Software Reference

The following table describes how command line interface syntax is shown in this Software Reference.

Syntax element	Example	What to enter in the command line

Keywords are shown in lowercase fixed-width font or bold variable-width font.	`show spanning-tree mst`
	or
	`show ip route`
		Some keywords are required, and others are optional parameters. Type keywords exactly as they appear in the command syntax.

Number ranges are enclosed in angle-brackets < > and separated by a hyphen.	*<0-255>*	Enter a number from the range. Do not enter the angle brackets.
Placeholders are shown in lowercase italics within angle-brackets < >, or in uppercase italics.	*<port-list>* or `ip dhcp pool` *NAME*	Replace the placeholder with the value you require. The placeholder may be an IP address, a text string, or some other value. See the parameter table for the command for information about the type of value to enter. Do not enter the angle-brackets.
Repeats are shown with ellipsis.	`param1...`	Enter the parameter one or more times.
Optional elements are shown in brackets: [ ]	`vlan` *<vid>* `[name` *<vlan-name>*`]`	If you need the optional parameter, enter it. Do not enter the brackets.
Required choices are enclosed in braces and separated by a vertical bar (pipe) : {|}	`spanning-tree {mstp|rstp|stp} enable`	Enter one only of the options. Do not enter the braces or vertical bar.
Optional choices are enclosed in or brackets and separated by a vertical bar (pipe): [|]	`[param1|param2]`	If needed, enter one only of the options. Do not enter the brackets or vertical bar.
Inclusive options are enclosed in braces, and separated by brackets: {[ ] [ ]}	`{[param1] [param2] [param3]}`	Enter one or more of the options and separate them with a space. Do not enter the braces or brackets.

Chapter 3: Start-Up Sequence

AlliedWare Plus Start-Up 3.2
Diagnostic Menu 3.3
Bootloader Menu 3.4
Start-Up Sequence 3.10

AlliedWare Plus Start-Up

Every switch has a start-up process. A specified version of product software must be loaded and executed. The bootloader is the executable code responsible for setting up the system and loading the release software.

The bootloader is the software that runs the unit when it first powers up, performing basic initialization and executing the product software release. As part of the start-up process of the switch, the bootloader allows you various options before running the product release software.

Previous versions of AlliedWare provide the option to boot to EPROM if a software release cannot be loaded or if selected by the user. The EPROM provides enough basic functionality to get a working software release loaded and operational on the switch. In AlliedWare Plus™ this task is handled by the bootloader.

As AlliedWare Plus™ begins its start-up process; there are two options that allow you to access either the diagnostic menu, or the bootloader menu. The following prompt is displayed when these options are temporarily available:

```
Bootloader 3.0.0-devel loaded
Press <Ctrl+B> for the Boot Menu
```

You can now enter one of the following two options to determine how the start-up process proceeds:

- Enter Ctrl+D to display the diagnostic menu.
- Enter Ctrl+B to display the bootloader menu.

Diagnostic Menu

Enter Ctrl+D during start-up to access the bootloader diagnostic menu, and provide options for performing various hardware tests. This can be useful as a tool for confirming a suspected hardware problem at the direction of network engineering personnel. When you enter Ctrl+D, the stage 1 diagnostics menu is displayed:

```
Bootup Stage 1 Diagnostics Menu:
  0. Restart
  1. Full RAM test
  2. Quick RAM test
  3. Battery backed RAM (NVS) test
  4. Bootloader ROM checksum test
  ---------------------------------
  7. Bootup stage 2 diagnostics menu
  ---------------------------------
  8. Quit to U-Boot shell
  9. Quit and continue booting
Enter selection ==>
```

The options in the stage 1 diagnostics menu allow you to initiate the following tests:

- **RAM:** The Bootloader fully tests any/all SDRAM installed in the system.
- **NVS:** The Bootloader fully tests any/all non-volatile (battery backed) SRAM installed in the system.
- **checksum:** The Bootloader checksum ROM memory for error detection.

For example, enter “2” to select a Quick RAM test:

```
Quick RAM test - press Q to quit, S to skip when failing
Writing pattern  ..............................
Checking pattern ..............................
Writing complemented pattern ..................
Checking complemented pattern ..................
Pass 1  total errors 0
```

Enter “7” to display the stage 2 diagnostics menu:

```
Entering stage 2...
Bootup Stage 2 Diagnostics Menu:
  0. Restart
  2. Test FLASH (Filesystem only)
  4. Erase FLASH (Filesystem only)
  5. Card slot test
  --------------------------------
  8. Quit to U-Boot shell
  9. Quit and continue booting
```

The options in the stage 2 diagnostics menu allow you to initiate the following tests:

- **Flash:** The Bootloader tests the user file system area of Flash. The bootloader is stored in a protected area of Flash that is not accessed by the user file system.
- **Flash Erase:** The Bootloader erases the user file system area of Flash only.

Once any required tests are completed from the diagnostics menu, enter “9” to quit the diagnostic menu and continue the switch boot-up process.

Bootloader Menu

Enter Ctrl+B during start-up to access the bootloader menu where boot options can be set. The boot options shown are explained in detail under this example.

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

Boot options

A powerful feature of AlliedWare Plus™ is the ability to boot from a variety of sources. Previously the switch was constrained to just booting off the release loaded into Flash memory. The only software release upgrade path being to load a new release into Flash memory and then set this release to be loaded at the next restart.

With AlliedWare Plus™ the switch can boot from other sources, such as a USB stick or network server. This provides a very flexible system, with multiple options to upgrade software releases and for system recovery.

Details of the bootloader menu options are as follows:

1. Perform one-off boot from alternate source

Enter "1" in the top-level menu to provide the following one-off boot options:

```
Enter selection ==> 1

Select device:

  0. Return to previous menu
  ------------------------------------------------------
  1. Flash    (flash:)
  2. TFTP     (tftp://)
  3. YMODEM   (ymodem:)
  4. USB      (usb:)

Enter selection ==>
```

You can select a one-off boot from Flash, USB storage device, network server (TFTP), or ymodem. The selected option will be used for the next restart (only) of the switch. If you select to boot from the network, the bootloader prompts the user for the required network address details.

Note These settings are specific to the Bootloader. They are not related in any way to what may be configured by the main software release.

```
Enter IP version [4|6]......... [4]:
  Enter IP address for eth0 ..... [0.0.0.0]: 172.28.8.210
  Enter subnet mask ............. [0.0.0.0]: 255.255.0.0
  Enter gateway IP .............. [0.0.0.0]: 172.28.0.1
  Enter TFTP server IP .......... [0.0.0.0]: 172.30.1.242
  Enter filename ................ []: GS900-5.4.4E-1.1.rel
Loading tftp://172.30.1.242/GS900-5.4.4E-1.1.rel...
```

When the switch is booted up using the 'one-off' selected source for the software release, it provides the option to copy the release just used to Flash for further/permanent use:

```
login: manager
Password: ******
The system has been booted using the one off boot/recovery
mechanism.
Bootup has successfully completed.
Write this release to flash? (y/n):
```

2. Change the default boot source (for advanced users)

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

Entering “2” in the top-level menu provides the option to set the boot source permanently.

```
Enter selection ==> 2

  NOTE: These settings are specific to the Bootloader.
  They are not related in any way to what may be configured
  by the 'boot system' command in the main software release.

Select device:

  0. Return to previous menu
  ------------------------------------------------------
  1. Flash    (flash:)
  3. TFTP     (tftp://)
  4. YMODEM   (ymodem:)
  6. USB      (usb:)
  ------------------------------------------------------
  9. Boot from default (determined by main CLI)

Enter selection ==> 1
```

The same boot source options are provided as with the one-off selection, but this time every restart of the switch will result in the unit booting from the selected source.

3. Update Bootloader

This option allows for the bootloader code to be updated. It is not detailed here, as it is envisioned that this would rarely need to be done, and only at the request of (and with support from) Allied Telesis engineering.

4. Adjust the console baud rate

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

The baud rate of the console session is set here to match the terminal program being used for management of the switch when connected directly to the asynchronous port. The switch's default value is 9600. The baud rate selected can be set as the 'new' default for future use if preferred.

```
Select baud rate:

  0. Return to previous menu
  ------------------------------------------------------
  1. 9600
  2. 19200
  3. 38400
  4. 57600
  5. 115200
  6. 230400 (Setting can't be made permanent)
  7. 460800 (Setting can't be made permanent)

Enter selection ==>  1

Change your terminal program baud rate to 9600 and press
enter...  if for some reason you are unable to do this,
power cycle the device and the existing baud rate will be
restored.
Use this baud rate by default? (Y/N) ==> n
```

5. Special boot options

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

The special boot options allow for system recovery in the event of a forgotten password or to the default configuration.

```
Special boot options menu:

  0. Return to previous menu
  ------------------------------------------------------
  1. Skip startup script (Use system defaults)

Enter selection ==>
```

6. System information

```
Boot Menu:

  WARNING: The bootloader is not currently password protected.
  ------------------------------------------------------
  B. Boot backup software
  ------------------------------------------------------
  S. Security Level
  ------------------------------------------------------
  0. Restart
  1. Perform one-off boot from alternate source
  2. Change the default boot source (for advanced users)
  3. Update Bootloader
  4. Adjust the console baud rate
  5. Special boot options
  6. System information
  7. Restore Bootloader factory settings
  ------------------------------------------------------
  9. Quit and continue booting

Enter selection ==>
```

The system information option provides some details on the hardware platform in use, such as CPU, memory, hardware (MAC) address and so on.

7. Restore Bootloader factory settings

This option allows the bootloader to be set back to factory defaults.

Caution

This option erases any settings that may have been configured by this menu
Are you sure? (Y/N) ==>

The bootloader menu provides a powerful set of options for flexibility in the way software releases are upgraded on the switch, and system recovery is performed.

Start-Up Sequence

The start-up sequence for a device running AlliedWare Plus™ under normal circumstances will be as seen in the following pages. This sequence will be seen when everything loads and runs as expected.

Note

To enter the bootloader or diagnostic menus discussed previously, Ctrl+B or Ctrl+D must be entered when prompted before the software modules start loading.

```
Reading flash:GS900-5.4.4E-1.1.rel...

Verifying release... OK
Booting...
Starting base/first...                                  [  OK  ]
Mounting virtual filesystems...                         [  OK  ]
           _______________   ____
        /\ \             / /______\
      /   \ \_      __/ /| ______ |
    /      \ |     |  /  | ______ |
  /         \ \   / /     \ ____ /
/______/\____\ \/ /____________/
Allied Telesis Inc.
AlliedWare Plus (TM) vVersion 5.4.4E-1
Current release filename: GS900-5.4.4E-1.1.rel
Original release filename: GS900-5.4.4E-1.1.rel
Built: Fri Feb 28 10:34:21 NZDT 2015
Mounting static filesystems...                          [  OK  ]
Checking flash filesystem...                            [  OK  ]
Mounting flash filesystem...                            [  OK  ]
Checking NVS filesystem...                              [  OK  ]
Mounting NVS filesystem...                              [  OK  ]
Starting base/dbus...                                   [  OK  ]
Starting base/syslog...                                 [  OK  ]
Starting base/loopback...                               [  OK  ]
Starting base/poe_done...                               [  OK  ]
Starting base/sysctl...                                 [  OK  ]
Starting base/portmapper...                             [  OK  ]
Received event syslog.done
Starting base/reboot-stability...                       [  OK  ]
Checking system reboot stability...                     [  OK  ]
Starting base/cron...                                   [  OK  ]
Starting base/appmond...                                [  OK  ]
Starting hardware/openhpi...                            [  OK  ]
Starting hardware/timeout...                            [  OK  ]
Starting base/inet...                                   [  OK  ]
Starting base/modules...                                [  OK  ]
Received event modules.done
Received event board.inserted
Starting network/poefw...                               [  OK  ]
Received event poefw.done
Received event hardware.done
Starting network/startup...                             [  OK  ]
Starting base/external-media...                         [  OK  ]
Starting network/stackd...                              [  OK  ]
Starting network/election.timeout...                    [  OK  ]
Received event network.enabled

Initializing HA processes:
hostd, cntrd, nsm, ripngd, sflowd, auth, epsr
hsl, imiproxyd, irdpd, lldpd, loopprot, mstp, ospf6d
pdmd, pim6d, ripd, rmon, vrrpd, atmfd, bgpd
lacp, ospfd, pimd, udldd, imi
Received event network.initialized
21:14:13 awplus-1 VCS[951]: No neighboring members found, unit may be in a stand
alone configuration
Received event vcs.elected-master
21:14:13 awplus-1 VCS[951]: Startup speed can be improved by adding 'no stack 1
enable' to configuration
21:14:13 awplus-1 VCS[951]: Member 1 (eccd.6d9d.4eed) has become the Active Mast
er
Assigning Active Workload to HA processes:
21:14:13 awplus VCS[951]: Stack Virtual MAC is 0000.cd37.0065
21:14:22 awplus ATMF[896]: host_eccd_6d9d_4eed has joined. 1 member in total.
authd, epsrd, hsl, irdpd, lacpd, lldpd, loopprotd
mstpd, nsm, rmond, sflowd, vrrpd, imi, imiproxyd
Received event network.activated

Loading configuration file flash:/default.cfg, please wait.
...
done!
Received event network.configured

awplus login: manager
Password:
```

```
Verifying release... OK
Booting...
Starting base/first...                                    [  OK  ]
Mounting virtual filesystems...                           [  OK  ]

           _______________   ____
        /\ \             / /______\
      /   \ \_      __/ /| ______ |
    /      \ |     |  /  | ______ |
  /         \ \   / /     \ ____ /
/______/\____\ \/ /____________/

Allied Telesis Inc.
AlliedWare Plus (TM) v0.0.0
Current release filename:Version 5.4.4E-1-0.1.rel
Original release filename: Version 5.4.4E-1-0.1.rel
Built: Thu May 29 01:32:38 NZST 2015
hwclock: settimeofday: Invalid argument
Mounting static filesystems...                            [  OK  ]
Checking flash filesystem...                              [  OK  ]
Mounting flash filesystem...                              [  OK  ]
Checking for last gasp debug output...                    [  OK  ]
Checking NVS filesystem...                                [  OK  ]
Mounting NVS filesystem...                                [  OK  ]
Starting base/dbus...                                     [  OK  ]
Starting base/syslog...                                   [  OK  ]
Starting base/loopback...                                 [  OK  ]
Starting base/poe_done...                                 [  OK  ]
Starting base/sysctl...                                   [  OK  ]
Starting base/portmapper...                               [  OK  ]
Received event syslog.done
Starting base/reboot-stability...                         [  OK  ]
Checking system reboot stability...                       [  OK  ]
Starting base/cron...                                     [  OK  ]
Starting base/appmond...                                  [  OK  ]
Starting hardware/openhpi...                              [  OK  ]
Starting hardware/timeout...                              [  OK  ]
Starting base/inet...                                     [  OK  ]
Starting base/modules...                                  [  OK  ]
Received event modules.done
Received event board.inserted
Received event hardware.done
Starting network/startup...                               [  OK  ]
Starting base/external-media...                           [  OK  ]
Starting network/stackd...                                [  OK  ]
Starting network/election.timeout...                      [  OK  ]
Received event network.enabled

Initializing HA processes:
hostd, auth, cntrd, epsr, hsl, imiproxyd, mstp
nsm, rmon, sflowd, atmfd, imi, irdpd, lacp
lldpd, loopprot, udldd

Received event network.initialized

Assigning Active Workload to HA processes:
00:01:26 awplus VCS[996]: Stack Virtual MAC is 0000.cd37.02ea
hsl, nsm, lacpd, loopprotd, mstpd, rmond, sflowd
authd, epsrd, irdpd, lldpd, imi, imiproxyd

Received event network.activated

Loading default configuration
.......

done!
Received event network.configured


GS900 login:
```

There are three possible status results displayed for each module loaded - OK, INFO, ERROR:

- OK means that the module has loaded correctly.
- INFO means that an error occurred, but the device is usable.
- ERROR means that an error occurred and device operation may be affected.

Additional specific information accompanies an INFO or ERROR status result. For example, if a corrupt release file was set as the startup release, the following error message would be seen:

```
Bootloader 3.0.0-devel loaded
Press <Ctrl+B> for the Boot Menu
Reading filesystem...
Error: Release filename is invalid (should be GS900-5.4.4E-1.1.rel)
Error: There is no backup release file set
Error: Boot failed. Please recover the system using the Boot Menu
Restarting...Bootloader 3.0.0-devel loaded
Press <Ctrl+B> for the Boot Menu
```

Whether an error message results in a case of the device being unusable will depend on the specific error and message, so will need to be dealt with on a case by case basis. If a software release has been corrupted, as shown on start-up, a new release may need to be loaded.

Chapter 4: CLI Navigation Commands

Command List 4.2
configure terminal 4.2
disable (Privileged Exec mode) 4.2
do 4.3
enable (Privileged Exec mode) 4.4
end 4.6
exit 4.6
help 4.7
logout 4.7
show history 4.8

Command List

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

configure terminal

This command enters the Global Configuration command mode.

Syntax `configure terminal`

Mode Privileged Exec

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

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

disable (Privileged Exec mode)

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

Syntax `disable`

Mode Privileged Exec

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

```
awplus# disable
awplus>
```

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

do

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

Syntax `do <command>`

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

Mode Any configuration mode

Example

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

enable (Privileged Exec mode)

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

Syntax `enable [<privilege-level>]`

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

Mode User Exec

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

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

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

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

```
awplus> enable
awplus#
```

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

```
awplus> enable 7

awplus#
```

Related Commands

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

end

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

Syntax `end`

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

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

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

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

exit

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

Syntax `exit`

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

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

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

Related Commands **disable (Privileged Exec mode)**
enable (Privileged Exec mode)
end

help

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

Syntax `help`

Mode All command modes

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

```
awplus# help
```

Output **Figure 4-1: Example output from the help command**

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

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

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

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

logout

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

Syntax `logout`

Mode User Exec and Privileged Exec

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

```
awplus# logout
```

show history

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

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show history`

Mode User Exec and Privileged Exec

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

```
awplus# show history
```

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

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

Chapter 5: User Access Commands

Introduction 5.2
Command List 5.2
clear line console 5.2
clear line vty 5.3
enable password 5.4
  Using plain passwords 5.5
  Using encrypted passwords 5.5
  Using hidden passwords 5.6
enable secret 5.7
  Using plain passwords 5.8
  Using encrypted passwords 5.8
  Using hidden passwords 5.9
exec-timeout 5.10
flowcontrol hardware (asyn/console) 5.11
length (asyn) 5.13
line 5.14
privilege level 5.16
security-password history 5.17
security-password forced-change 5.18
security-password lifetime 5.19
security-password minimum-categories 5.20
security-password minimum-length 5.21
security-password reject-expired-pwd 5.22
security-password warning 5.23
service advanced-vty 5.24
service http 5.25
service password-encryption 5.26
service telnet 5.27
show privilege 5.28
show security-password configuration 5.29
show security-password user 5.30
show telnet 5.31
show users 5.32
telnet 5.33
telnet server 5.34
terminal length 5.35
terminal resize 5.36
username 5.37

Introduction

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

Command List

clear line console

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

Syntax `clear line console 0`

Mode Privileged Exec

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

```
awplus# clear line console 0

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

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

clear line vty

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

Syntax

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

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

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

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

Related Commands

privilege level
line
show telnet
show users

enable password

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

Using plain passwords

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

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

This results in the following show output:

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

Using encrypted passwords

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

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

This results in the following show output:

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

Using hidden passwords

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

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

This results in the following show output:

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

Related Commands

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

enable secret

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

Using plain passwords

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

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

This results in the following show output:

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

Using encrypted passwords

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

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

This results in the following show output:

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

Using hidden passwords

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

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

This results in the following show output:

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

Related Commands

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

exec-timeout

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

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

Syntax

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

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

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

Mode Line Configuration

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

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

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

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

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

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

Validation Commands **show running-config**

Related Commands **line**
service telnet

flowcontrol hardware (asyn/console)

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

Syntax

```
flowcontrol hardware
no flowcontrol hardware
```

Mode Line Configuration

Default Hardware flow control is disabled by default.

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

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

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

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

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

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

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

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

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

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

Related Commands

clear line console
show running-config
speed (asyn)

length (asyn)

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

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

Syntax

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

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

Mode Line Configuration

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

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

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

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

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

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

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

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

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

Related Commands **terminal length**
terminal resize

line

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

Syntax

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

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

Mode Global Configuration

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

To change the console (asyn) port speed, use this **line** command to enter Line Configuration mode before using the **speed (asyn)** command on page 8.66. Set the console speed (Baud rate) to match the transmission rate of the device connected to the console (asyn) port on your switch.

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

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

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

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

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

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

Related Commands

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

privilege level

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

Syntax `privilege level <1-15>`

Mode Line Configuration

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

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

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

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

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

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

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

Related Commands **enable password**
line
show privilege
username

security-password history

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

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

Syntax

```
security-password history <0-15>

no security-password history
```

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

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

Mode Global Configuration

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

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

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

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

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

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

security-password forced-change

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

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

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

Syntax

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

Default The forced-change feature is disabled by default.

Mode Global Configuration

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

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

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

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

security-password lifetime

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

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

security-password minimum-categories

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

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

security-password minimum-length

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

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

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

Default The default minimum password length is `1`.

Mode Global Configuration

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

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

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

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

security-password reject-expired-pwd

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

Caution

Once all users' passwords are expired you are unable to login to the device again if the security-password reject-expired-pwd command has been executed. You will have to reboot the device with a default configuration file, or load an earlier software version that does not have the security password feature.
We recommend you never have the command line "security-password reject-expired-pwd" in a default config file.

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

security-password warning

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

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

service advanced-vty

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

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

Syntax

```
service advanced-vty
no service advanced-vty
```

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

Mode Global Configuration

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

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

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

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

service http

This command enables the HTTP (Hypertext Transfer Protocol) service. The HTTP service is enabled by default.

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

Syntax

```
service http
no service http
```

Default The HTTP service is enabled by default.

Mode Global Configuration

Examples To disable the HTTP service, use the command:

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

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

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

service password-encryption

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

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

Syntax

```
service password-encryption
no service password-encryption
```

Mode Global Configuration

Example

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

Validation Commands show running-config

Related Commands enable password

service telnet

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

The server listens on port 23, unless you have changed the port by using the **privilege level** command on page 5.16.

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

Syntax

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

Default The IPv4 and IPv6 telnet servers are enabled by default.

The configured telnet port is TCP port 23 by default.

Mode Global Configuration

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

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

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

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

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

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

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

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

Related Commands

clear line vty
show telnet
telnet server

show privilege

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

Syntax `show privilege`

Mode User Exec and Privileged Exec

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

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

```
awplus# show privilege
```

Output **Figure 5-1: Example output from the show privilege command**

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

Related Commands privilege level

show security-password configuration

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

Syntax `show security-password configuration`

Mode Privileged Exec

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

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

Output **Figure 5-2: Example output from the show security-password configuration command**

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

Related Commands **show running-config security-password**
show security-password user

show security-password user

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

Syntax `show security-password user`

Mode Privileged Exec

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

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

Output **Figure 5-3: Example output from the show security-password user command**

```
User account and password information

UserName          Privilege Last-PWD-Change   Remaining-lifetime
------------------------------------------------------------------
manager           15          4625 day(s) ago   No Expiry
bob15             15             0 day(s) ago   30 days
ted7              7              0 day(s) ago   No Expiry
mike1             1              0 day(s) ago   No Expiry
```

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

show telnet

This command shows the Telnet server settings.

Syntax `show telnet`

Mode User Exec and Privileged Exec

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

```
awplus# show telnet
```

Output **Figure 5-4: Example output from the show telnet command**

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

Related Commands
clear line vty
service telnet
show users
telnet server

show users

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

Syntax `show users`

Mode User Exec and Privileged Exec

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

```
awplus# show users
```

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

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

Table 5-1: Parameters in the output of the show users command

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

telnet

Use this command to open a telnet session to a remote device.

Syntax `telnet {<hostname>|[ip] <ipv4-addr>|[ipv6] <ipv6-addr>} [<port>]`

Parameter	Description
<hostname>	The host name of the remote system.
`ip`	Keyword used to specify the IPv4 address or host name of a remote system.
<ipv4-addr>	An IPv4 address of the remote system.
`ipv6`	Keyword used to specify the IPv6 address of a remote system
<ipv6-addr>	Placeholder for an IPv6 address in the format `x:x::x:x`, for example, `2001:db8::8a2e:7334`
<port>	Specify a TCP port number (well known ports are in the range 1-1023, registered ports are 1024-49151, and private ports are 49152-65535).

Mode User Exec and Privileged Exec

Examples To connect to TCP port `2602` on the device at `10.2.2.2`, use the command:

```
awplus# telnet 10.2.2.2 2602
```

To connect to the telnet server `host.example`, use the command:

```
awplus# telnet host.example
```

To connect to the telnet server `host.example` on TCP port `100`, use the command:

```
awplus# telnet host.example 100
```

telnet server

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

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

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

Mode Global Configuration

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

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

Related Commands **show telnet**

terminal length

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

Use the **terminal no length** command to remove the length specified by this command. The default length will apply unless you have changed the length for some or all lines by using the **length (asyn)** command on page 5.13.

Syntax

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

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

Mode User Exec and Privileged Exec

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

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

Related Commands

length (asyn)
terminal resize

terminal resize

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

Syntax `terminal resize`

Mode User Exec and Privileged Exec

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

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

```
awplus# terminal resize
```

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

username

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

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

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

Chapter 6: Creating and Managing Files

Introduction 6.2
USB Support 6.2
Working with Files 6.2
- Listing Files 6.3
- Displaying the Contents of Configuration and Text Files 6.4
- Navigating Through the File System 6.4
- Using the Editor 6.6

Creating and Using Configuration Files 6.8
- Creating a Configuration File 6.8
- Specifying the Start-Up Configuration Script 6.8
- Working with Configuration Files 6.9
- The Configuration File Fallback Order 6.10

Copying Files to and from Your Device 6.12
- URL Syntax 6.12
- Copying Files 6.13
- Copying from a Server to Running Configuration 6.17

The Autoboot Feature 6.19
- Restoring a Switch Using Autoboot from External Media 6.20
- Configure Autoboot 6.22

Introduction

This chapter provides information on:

- **USB Support**
- **Working with Files**
- **Creating and Using Configuration Files**
- **Copying Files to and from Your Device**

USB Support

Your switch supports both standard and secure USB storage devices.

USB storage devices used as backup memory can be easily pulled out of a switch. You can use Secure USB storage devices to protect this data in the event that it is mislaid or in unauthorized hands. Secure USB devices provide password (PIN)-protected encryption to the data they store.

Note that if the switch reboots, the Secure USB key will be locked.

After a VCStack failover, when a stack member recovers, the Secure USB device cannot be accessed until it is unlocked.

Working with Files

The AlliedWare Plus™ OS lets you create directory trees for file storage. This section shows:

- **"Listing Files" on page 6.3**—listing files and seeing how much free space you have
- **"Displaying the Contents of Configuration and Text Files" on page 6.4**
- **"Navigating Through the File System" on page 6.4**—identifying the current directory, changing directories, and creating and deleting directories
- **"Using the Editor" on page 6.6**

Flash compaction

The Flash memory on the switch automatically compacts itself to recover space available from deleted files. The switch only does this when necessary, and not every file deletion causes Flash compaction. Flash compaction can occur after a file of any size is added to or deleted from the switch.

Caution While Flash is compacting, the console is unresponsive. Do not restart the switch, as interrupting Flash compaction can damage files.

Listing Files

To list files, enter Privileged Exec mode and enter the command:

```
awplus# dir
```

The output lists files and directories in order of modification date, descending. It looks like this:

```
-rw-      534 Jul 12 2014 17:52:50  stp.cfg
-rw-      534 Jul 12 2014 17:12:50  example.cfg
-rw- 12429011 Jul 12 2014 16:26:06  GS900-5.4.4E-1.1.rel
```

Listing files including hidden system files

The **dir** command does not list all files—it hides system files and directories because users generally do not need to create or edit them. To list all files including system files, enter Privileged Exec mode and enter the command:

```
awplus# dir all
```

The output looks like this:

```
drwx        0 Jul 12 2011 17:16:32  ./
-rw-      401 Jul 12 2011 17:16:32  example.cfg
-rw-      534 Jul 12 2011 17:52:50  stp.cfg
-rw- 12429011 Jul 12 2011 16:26:06  GS900-5.4.4E-1.1.rel
drwx      216 Jul  9 2011 11:31:18  ../
drwx        0 Jun 13 2011 04:31:51  .configs/
-rw-       17 Jun 13 2011 04:27:27  .release
drwx        0 Jul 10 2011 23:40:00  .ssh/
```

The hidden files and directories begin with a dot.

Seeing information about the filesystem

To display information about the different memory types on the switch, enter Privileged Exec mode and enter the command:

```
awplus# show file systems
```

The output includes the amount of free memory and the prefix you type to access that memory type, and looks like this:

```
 Size(b)  Free(b)  Type   Flags  Prefixes   S/D/V   Lcl/Ntwk  Avail
-------------------------------------------------------------------
 126.0M   106.4M   flash     rw  flash:     static  local      Y
      -        -   system    rw  system:    virtual local      -
  10.0M     9.8M   debug     rw  debug:     static  local      Y
 499.0K   404.0K   nvs       rw  nvs:       static  local      Y
      -        -   usbstick  rw  usb:       dynamic local      N
      -        -   tftp      rw  tftp:      -       network    -
      -        -   scp       rw  scp:       -       network    -
      -        -   sftp      ro  sftp:      -       network    -
      -        -   http      ro  http:      -       network    -
```

Listing files in a subdirectory

To list the contents of a directory, enter Privileged Exec mode and enter the command:

```
awplus# dir <directory-name>
```

Tip You can specify the directory with or without a / after the directory name.

Example To display the contents of a directory called “example”, enter the command:

```
awplus# dir example
```

Listing files in NVS memory or on a USB storage device

To list the contents of a directory on a USB storage device, enter the command:

```
awplus# dir usb:<directory-name>
```

Example To display the contents of a directory in NVS called “example”, enter the command:

```
awplus# dir nvs:example
```

Displaying the Contents of Configuration and Text Files

To display the contents of a file, enter Privileged Exec mode and enter the command:

```
awplus# show file <filename>
```

Example To display the contents of the file called “example.cfg”, enter the command:

```
awplus# show file example.cfg
```

Navigating Through the File System

Showing the current directory

To see which directory you are currently in, enter Privileged Exec mode and enter the command:

```
awplus# pwd
```

For the top-level directory, the output looks like this:

```
flash:/
```

Changing directories

To change to another directory, enter Privileged Exec mode and enter the command:

```
awplus# cd <directory-name>
```

To go to a directory one level higher in the directory tree, enter the command:

```
awplus# cd ..
```

Example To change to a directory called “example”, enter the command:

```
awplus# cd example
```

To go up one level, which returns you to the top level directory, enter the command:

```
awplus# cd ..
```

Changing to a directory in NVS memory or on a USB storage device

To change to the top-level directory in the NVS memory filesystem, enter Privileged Exec mode and enter the command:

```
awplus# cd nvs:
```

To change to the top-level directory on a USB storage device, enter the command:

```
awplus# cd usb:/
```

Next, you can change to other directories by entering the command:

```
awplus# cd <directory-name>
```

Alternatively, you can go straight from Flash to a subdirectory in the alternative filesystem, by entering one of the commands:

```
awplus# cd nvs:<directory-name>
```

```
awplus# cd usb:/<directory-name>
```

To return to the Flash filesystem, enter the command:

```
awplus# cd flash:/
```

Example To change to the directory within NVS called “example”, enter the command:

```
awplus# cd nvs:example
```

To go up one level, which returns you to the top-level directory of NVS memory, enter the command:

```
awplus# cd ..
```

Creating new directories

To create a directory, enter Privileged Exec mode and enter the command:

```
awplus# mkdir <directory-name>
```

Example To make a directory called “example” within the Flash filesystem, enter the command:

```
awplus# mkdir example
```

Deleting directories

To delete an empty directory, enter Privileged Exec mode and enter the command:

```
awplus# rmdir <directory-name>
```

To delete a directory and all its contents, enter Privileged Exec mode and enter the command:

```
awplus# delete recursive <directory-name>
```

The switch prompts you for confirmation.

Example To delete an empty directory called “example” from within the Flash filesystem, enter the command:

```
awplus# rmdir example
```

Using the Editor

The inbuilt editor is JOE (Joe’s Own Editor).

To edit an existing file, enter Privileged Exec mode and enter the command:

```
awplus# edit <filename>
```

To open the editor with an empty file, enter the command:

```
awplus# edit
```

When you save the new file, you may need to specify the filesystem to store it on. For Flash, use **flash:/<*filename*>**.

Using JOE To format and manipulate text in JOE, you use control-character sequences. The following table summarizes a few useful sequences—for details, see:

joe-editor.sourceforge.net/manpage.html.

Function	Control-character sequence
Access the help	Ctrl-K-H
Save the file without exiting (for new files, this prompts for a filename)	Ctrl-K-D
Save the file and exit (this prompts for a filename)	Ctrl-K-X
Exit without saving the file	Ctrl-C
Go to the beginning of the file	Ctrl-K-U
Go to the end of the file	Ctrl-K-V
Go up one full screen of text in the file	Ctrl-U
Go down one full screen of text in the file	Ctrl-V
Select a block of text:	
Mark the beginning of the block	Ctrl-K-B
Mark the end of the block	Ctrl-K-K
Copy and paste a selected block of text	Place cursor at destination then enter Ctrl-K-C
Move a selected block of text	Place cursor at destination then enter Ctrl-K-M
Delete a selected block of text	Ctrl-K-Y

Creating and Using Configuration Files

This section provides instructions on:

- **Creating a Configuration File**
- **Specifying the Start-Up Configuration Script**
- **Working with Configuration Files**

Creating a Configuration File

A **configuration file** is a text file that contains a sequence of standard commands for a specific purpose. Configuration files have a **.cfg** extension.

You can create and edit configuration files on your device by:

- saving the dynamic configuration on the device, known as the **running-config** (see **"Working with Configuration Files"**). Use the command:

```
awplus# copy running-config (destination-URL)
```

  where URL specifies a file in Flash. If you do not specify a file name, the switch names the file **default.cfg**.

- using the device's text editor. Use the command:

```
awplus# edit (source-URL)
```

  where **source-URL** is the name of the copied file in Flash memory.

- creating a file on a remote PC, then copying it to onto your device. See **"Copying Files"** for more information about using the **copy** commands.

Once you have created a configuration file, you can use it as the **startup-config** file. See **"Specifying the Start-Up Configuration Script"** for more information.

Specifying the Start-Up Configuration Script

When you restart your device, or when it automatically restarts, it executes the pre-configured commands in a configuration script known as the **boot config** or **startup-config** file.

When you first start your device, the script set as the startup-config file is **default.cfg**. If desired, you can overwrite **default.cfg** with another configuration. Alternatively, you can change the startup-config by specifying a new file as the startup-config. Use the command:

```
awplus(config)# boot config-file backup URL
```

where **URL** specifies the name and location of a configuration file. At the next restart, the device executes the commands in the specified file.

You can specify that the configuration file is either in the Flash or USB storage device filesystem. However, if you specify that the configuration file is on a USB storage device then you must first create a backup configuration file stored in Flash.

To specify a backup configuration file, use the command:

```
awplus(config)# boot config-file backup backup URL
```

where **URL** specifies the name and location of a configuration file.

You can change the content of the file set as the startup-config file by:

- entering commands directly into the CLI, then saving this configuration using the command:

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

  This command saves the device's dynamic configuration into the file that is currently configured as the startup-config file.

- writing commands into a configuration file (see **"Creating a Configuration File"** below), then using the command:

  ```
  awplus# copy SOURCE-URL startup-config
  ```

  This command saves the script from the source file into the file that is currently configured as the startup-config file.

To display the name of the configuration file that is set to execute when the device restarts, enter the command:

```
awplus# show boot
```

To see the commands in the startup-config file, use the command:

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

To erase the file set as the startup-config file, use the command:

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

At the next restart that occurs after you've erased the file, the device loads the configuration in the file **default.cfg**. This file is set on the system as a backup configuration file that loads if no other file is set as the startup-config file.

Working with Configuration Files

When you use the CLI to configure your device, it stores this dynamic configuration as a list of commands called the **running-config**. To view the device's running-config, use the command:

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

If you turn off the device or restart it, any unsaved changes to the running-config are lost. To save the running-config as a configuration script, use the command:

```
awplus# copy running-config destination-url
```

You may have many configuration files. Storing them on a device allows you to keep a backup device with configuration scripts for every device in the network to speed up network recovery time. Multiple scripts also let you test new configuration scripts before setting them as the startup-config. For example, to test a new script named test.cfg, enter the command:

```
awplus# copy flash:/test.cfg running-config
```

This allows you to run a configuration file any time without restarting the device, by replacing the system's current dynamic configuration with the script in the configuration file. However, note that some commands require you to restart the device before they can take effect, such as the **platform** commands.

You can also set a trigger to automatically execute a configuration script when a predetermined event occurs. For information about creating triggers, see **Chapter 74, Triggers Introduction**.

The Configuration File Fallback Order

The configuration fallback order is: configuration file, backup configuration file, default configuration file and then the factory default configuration. It is important to note the there is a distinction in system behavior between when writing to the startup-config file and when the system boots up.

When you copy a configuration script from a source file into the startup-config file the system will write to the first file that is configured. Potentially, this means that if a configuration file and a backup configuration file are not set you will write to the default.cfg.

At system startup the device goes through the fallback sequence until it finds a file that exists. For example, if the configuration file is not found then the backup configuration file becomes the current boot configuration, or startup-config, and so on. In the output displayed by the **show boot** command, the **Current boot config** parameter shows the startup-config file that the switch will load during the next boot cycle. The fallback sequence when configuration files are deleted is shown below in output from the **show boot** command.

In the example output below, the current boot configuration file, **my.cfg**, is set on the USB storage device. This is the startup-config file that the device loads at the next boot cycle.

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : usb:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file exists)
```

In the example output below, the **no boot-config** command has been used to delete the configuration file **my.cfg** on the USB storage device. The backup configuration file **backup.cfg** in Flash then becomes the current boot config.

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : usb:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/backup.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file exists)
```

In the example output below, the **no boot-config backup** command has been used to delete the backup configuration file **backup.cfg**. The default configuration file **default.cfg** then becomes the current boot config.

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rell
Current boot image : usb:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/default.cfg (file exists)
Backup  boot config: Not set
```

If the current boot configuration file is set on a USB storage device and this device has been removed from the switch, the **Current boot config** parameter field indicates that this file cannot be found, as shown in the following example output.

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : usb:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file not found)
Backup  boot config: flash:/backup.cfg (file exists)
```

At system startup the switch will load the backup configuration file as the startup-config.

Copying Files to and from Your Device

This section provides instructions on:

- **URL Syntax**
- **Copying Files**

URL Syntax

Many of the file management commands use the placeholder "URL" to represent the name and location of the file that you want to act on. The following table explains the syntax of this URL for each different type of file location.

When you copy a file...	Use this syntax:	Example:
Copying in local Flash memory	`flash:[/][<directory>/]<filename>`	To specify a file in the configs directory in Flash: `flash:configs/example.cfg`
Copying to or from a USB storage device	`usb:[/][<directory>/]<filename>`	To specify a file in the top-level directory of the USB stick: `usb:example.cfg`
Copying with Hypertext Transfer Protocol (HTTP)	`http://[[<username>:<password>]@] {<hostname>|<host-ip>}[/<filepath>]/<filename>`	To specify a file in the configs directory on the server: `http://www.company.com/configs/example.cfg`
Copying with Trivial File Transfer Protocol (TFTP)	`tftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: `tftp://172.1.1.1/example.cfg`
Copying with Secure Copy (SCP)	`scp://<username>@<location>[/<directory>][/<filename>]`	To specify a file in the configs directory on the server, logging on as user "bob": `e.g. scp://bob@10.10.0.12/configs/example.cfg`
Copying with SSH File Transfer Protocol (SFTP)	`sftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: `sftp://10.0.0.5/example.cfg`
Copying to or from stack member Flash	`<hostname>-<stack_ID>/flash:[/][<directory>/]<stack_member_filename>`	To specify a file in the configs directory on member 2 of a stack named vcstack: `vcstack-2/flash:/configs/example.cfg`

The URL can include characters from up to four categories. The URL categories are:

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

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

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

Copying Files

To copy files, use the **copy** commands. These commands allow you to copy files:

- between different memory types attached to your device. Use the command:

  ```
  awplus# copy <local-source> <local-destination> <filename>
  ```

  See **"Copying within a filesystem"** and **""** for further details.
- across a serial connection using ZMODEM. Use the command:

  ```
  awplus# copy zmodem
  ```

  See **"Copying with ZMODEM"** for further details.

- from your device onto a remote device, or to your device from a remote device. To copy a file across an interface with IP configured, use the command:

```
awplus# copy SOURCE-URL DESTINATION-URL
```

To copy files across these interfaces you can use the following protocols:

- **"Copying with Hypertext Transfer Protocol (HTTP)"**
- **"Copying with Trivial File Transfer Protocol (TFTP)"**
- **"Copying with Secure Copy (SCP)"**
- **"Copying with SSH File Transfer Protocol (SFTP)"**

Copying within a filesystem

Within a directory

To copy a file within the same directory, enter Privileged Exec mode and enter the command:

```
awplus# copy <source-filename> <destination-filename>
```

If the file already exists, the switch asks whether to overwrite it, with a message like this:

```
Overwrite flash:/example.cfg? (y/n)[n]:
```

To overwrite, press the "y" key then the Enter key.

Between directories

To copy a file to another directory within the same filesystem, enter the command:

```
awplus# copy <source-filename> <directory-name>
```

The / after the directory name is required. Otherwise the switch displays an error ("37: Destination file is a directory").

The switch then prompts you for the destination filename. To give the copy a new name, type the name at the prompt. You can include directory names in the path.

To use the same filename as the original, press the Enter key (do not press the "y" key—that names the copy "y").

Example

To put a copy of example.cfg into the example directory, enter the command:

```
awplus# copy example.cfg example/
```

The prompt and messages look like this:

```
Enter destination file name [example.cfg]:
Copying from source file, please wait...
Copying to destination file, please wait...
0: Successful operation
```

Copying to and from NVS or a USB storage device

In a stacked environment you can only access `flash` and `nvs` using the stack member file path. To access a USB storage device on a backup stack member, use the **remote-login** command on page 82.5.

To copy between filesystems, you need to specify the filesystem prefix (`nvs:` or `usb:`).

For example, to copy from Flash to NVS when your current directory is the top-level Flash directory, enter Privileged Exec mode and enter the command:

```
awplus# copy <source-filename> nvs:sd:
```

For example, to copy from Flash to the USB storage device when your current directory is the top-level Flash directory, enter Privileged Exec mode and enter the command:

```
awplus# copy <source-filename> usb:
```

The switch prompts you for the filename, as described in the previous section.

To copy from NVS to Flash when your current directory is the top-level Flash directory, enter the command:

```
awplus# copy nvs:<source-filename> <destination-filename>
```

Example To copy the file “example.txt” from the directory called “example” in NVS, to the top level of Flash, enter the command:

```
awplus# copy nvs:example/example.txt example.txt
```

Copying with ZMODEM

ZMODEM allows you to copy files from a network host over an asynchronous port. Use the command:

```
awplus# copy zmodem
```

to open Minicom and transfer a file. Alternatively you can specify the file name within the command:

```
awplus# copy SOURCE-URL zmodem
```

For example, to copy the file “july.cfg” from Flash memory using ZMODEM, use the command:

```
awplus# copy flash:/july.cfg zmodem
```

Copying with Hypertext Transfer Protocol (HTTP)

You device has a built-in HTTP client. The HTTP client enables the device to act as a browser by sending HTTP “get” or “post” requests to an HTTP server. The client is enabled by default.

For example, to load the file “bob.key” onto Flash from the security directory on the web server at www.company.com, use the command:

```
awplus# copy http://www.company.com/security/bob.key
       flash:/bob.key
```

Copying with Trivial File Transfer Protocol (TFTP)

TFTP runs over User Datagram Protocol (UDP). It is simpler and faster than FTP but has minimal capability, such as no provisions for user authentication.

To copy a file from a TFTP server to Flash memory, enter Privileged Exec mode and enter the command:

```
awplus# copy tftp flash
```

Note

You can specify the server and filename in the command instead of waiting for prompts. Use a format like the following:

```
copy tftp://172.1.1.1/example.cfg flash
```

The switch prompts you for the:

- TFTP server hostname (you can enter its IP address instead)
- source filename on the TFTP server
- destination filename in Flash on the switch

To copy a file from Flash to a TFTP server, enter the command:

```
awplus# copy flash tftp
```

Follow the prompts for source filename, server, and destination filename.

If the file is not in the top level of the TFTP server, include the path as part of the filename.

Example To copy example.cfg to the TFTP server at 172.1.1.1, enter the command:

```
awplus# copy flash tftp
```

The prompts, responses, and messages look like this:

```
Enter source file name []:example.cfg
Enter destination host name []:172.1.1.1
Enter destination file name [example.cfg]:
Copying from source file, please wait...
Copying to destination file, please wait...
0: Successful operation
```

To load the file “bob.key” from a TFTP server, where the file is in the folder “security”, use the command:

```
awplus# copy tftp://security/bob.key flash:/bob.key
```

Copying with Secure Copy (SCP)

Secure Copy (SCP) provides a secure way to copy files to and from a remote device using SSH. The AlliedWare Plus™ OS includes both a SSH server and a SSH client. You must enable the SSH server before your device accepts connections from SCP clients. See the **Chapter 52, Secure Shell (SSH) Introduction** for more information.

For example, to load the file “beth.key” onto Flash from the key directory on a remote SSH server at 10.10.0.12, using the username “bob”, use the command:

```
awplus# copy scp://bob@10.10.0.12/key/beth.key
       flash:/beth.key
```

Copying with SSH File Transfer Protocol (SFTP)

SSH File Transfer Protocol (SFTP) provides a secure way to copy files onto your device from a remote device. The AlliedWare Plus™ OS includes both a SSH server and a SSH client. SFTP provides additional features from SCP, such as allowing you to manipulate the remote files, and halt or resume file transfers without closing the session.

For example, to load the file “rei.cfg” onto Flash memory from the remote server at 10.0.0.5, use the command:

```
awplus# copy sftp://10.0.0.5/rei.cfg flash:/rei.cfg
```

Copying from a Server to Running Configuration

Use the **copy tftp** variant of the **copy running-config** command on page 7.14 to load a configuration file from a server to the running configuration of the switch.

The configuration will be added to the running configuration as if the commands were typed in the command line interface.

The resulting configuration file will be a combination of the previous running configuration and the loaded configuration file. The loaded configuration file has precedence.

The Autoboot Feature

The Autoboot feature enables your switch to automatically load a specific release file and/or configuration file from external media, such as USB storage device, into Flash memory, providing there is enough free space available.

If there is not enough free space, the Autoboot feature will exit and booting will revert to what was previously set by the CLI. This feature is enabled only the first time the device is powered up in the field. Subsequently, the Autoboot feature is disabled by default.

The Autoboot feature minimizes network downtime by avoiding the need for manual configuration of a replacement device.

If you use prepared external media for the first time boot, the Autoboot feature gives you the ability to easily ensure the device boots with your desired release and configuration files. You must prepare the external media for this purpose using an initiation file, `autoboot.txt`, and accompanying release and configuration files.

Use the **create autoboot** command to create an `autoboot.txt` file on external media. This command will automatically ensure that the keys and values that are expected in this file are correct. After the file is created the command will copy the current release and configuration files across to the external media. The `autoboot.txt` file is read/writable by any desktop operating system currently supported by the AlliedWare Plus™ Operating System. Note that the external media file system is not case sensitive.

When the Autoboot feature is enabled, the device on boot-up:

- checks for a special file called `autoboot.txt` on external media, and if this file exists,
- checks in the file for the "key=value" pair "`Copy_from_external_media_enabled=yes`", and if this enable flag is set,
- loads the release file and/or configuration file from external media.

An example of a valid `autoboot.txt` file is shown in **Figure 6-1** below.

Figure 6-1: Example autoboot.txt file

```
; J Smith,  GS948MX,  14 May 2015
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=GS900-5.4.4E-1.1.rel
Boot_Config=network1.cfg
```

We recommend that no directories are present on external media used to hold the `autoboot.txt` file. In addition, large numbers of files on external media may slow the booting process.

Note The Autoboot feature is not supported in a stacked configuration.

Do not remove external media part way through the copy process as this may leave the device in an unstable state.

Configuration files placed on external media reduce security. Therefore, ensure adequate security precautions are taken with external media holding configuration files.

Restoring a Switch Using Autoboot from External Media

The example below describes the sequence of events when a switch in the field fails and is restored using this feature:

1. Using the **create autoboot** command, a network engineer has previously manually created a restore external media device, such as a USB storage device. The external media device contains the following components:
   - An `autoboot.txt` file with required contents
   - An appropriate release file
   - A configuration file
2. A switch fails in the field.
3. A replacement switch of same model is installed.
4. The previously created external media device is placed into the replacement switch.
5. The switch powers up using its pre-installed release if present. It automatically checks the external media device for the `autoboot.txt` file.
6. The switch finds a valid `autoboot.txt` file on the external media device, with the value “Copy_from_external_media_enabled” set. The release file and configuration file both exist on the external media device.
7. The MD5sum of pre-installed Flash release file is compared to the MD5sum of the release file stored in the external media device. If they do not match, because the release file in the replacement switch is either missing or different, then the release is restored from the external media device. If the release files already match, then the release file is not copied from the external media device.
8. The MD5sum of the Flash configuration file `default.cfg` (if pre-installed in the replacement switch) is compared to the MD5sum of the configuration file stored in the external media device. If they do not match, because the configuration file in the replacement switch is either missing or different, then the configuration file is restored from the external media device. If the configuration files already match, then the configuration file is not copied from the external media device.
9. The memory space available in the switch Flash is checked to ensure the release and configuration files stored in the external media device will fit. If there is not enough space the Autoboot feature will exit.
10. The release file and configuration files are automatically copied from the external media device to switch Flash memory. The switch release and configuration files are updated to contain the appropriate names.
11. The switch is automatically rebooted.
12. The replacement switch is now running the restored release and configuration files. Subsequent reboots are based on the restored release and configuration files stored in the switch Flash memory.

13. If you want to Autoboot from external media on this specific switch in the future, you must now manually enable the Autoboot feature in the configuration menu via the **autoboot enable** command. This command resets the enable flag stored internally in the switch NVS memory.

Configure Autoboot

This section describes the commands used to configure the Autoboot feature.

Table 6-1: Configuration procedures for the Autoboot feature

Create an Autoboot file (autoboot.txt)	
`awplus#`	
`create autoboot [usb]`	Create an **autoboot.txt** file on external media.
Enable the Autoboot feature	
`awplus#`	
`configure terminal`	Enter Global Configuration mode.
`awplus(config)#`	
`autoboot enable`	The Autoboot feature is enabled by default the first time the device is powered up in the field. Use this command to enable the feature subsequently.
Disable the Autoboot feature	
`awplus(config)#`	
`no autoboot enable`	Use this command to disable the Autoboot feature.
Display Autoboot configuration and status	
`awplus#`	
`show autoboot`	Display detailed information about the current Autoboot configuration and status.
`awplus#`	
`show boot`	Display the status of the Autoboot feature; either enabled or disabled.

Chapter 7: File Management Commands

Introduction 7.3
URL Syntax and Keyword Usage 7.3
Command List 7.5
autoboot enable 7.5
boot config-file 7.6
boot config-file backup 7.8
boot system 7.9
boot system backup 7.11
cd 7.12
copy current-software 7.12
copy debug 7.13
copy running-config 7.14
copy startup-config 7.15
copy (URL) 7.16
copy zmodem 7.18
create autoboot 7.19
delete 7.20
delete debug 7.21
dir 7.22
edit 7.24
edit (URL) 7.25
erase startup-config 7.26
mkdir 7.27
move 7.28
move debug 7.29
pwd 7.30
rmdir 7.31
show autoboot 7.32
show boot 7.33
show file 7.35
show file systems 7.36
show running-config 7.38
show running-config access-list 7.40
show running-config as-path access-list 7.41
show running-config dhcp 7.42
show running-config full 7.43
show running-config interface 7.44
show running-config ip route 7.46
show running-config ipv6 access-list 7.47
show running-config ipv6 route 7.48
show running-config key chain 7.49
show running-config lldp 7.50
show running-config power-inline 7.51
show running-config route-map 7.52
show running-config router 7.53
show running-config router-id 7.54
show running-config security-password 7.55

show startup-config 7.56
show version 7.57
write file 7.58
write memory 7.58
write terminal 7.58

Introduction

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

URL Syntax and Keyword Usage

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

When you copy a file...	Use this syntax:	Example:
Copying in local Flash memory	`flash:[/][<directory>/]<filename>`	To specify a file in the configs directory in Flash: `flash:configs/example.cfg`
Copying to or from a USB storage device	`usb:[/][<directory>/]<filename>`	To specify a file in the top-level directory of the USB stick: `usb:example.cfg`
Copying with Hypertext Transfer Protocol (HTTP)	`http://[[<username>:<password>]@] {<hostname>|<host-ip>}[/<filepath>]/<filename>`	To specify a file in the configs directory on the server: `http://www.company.com/configs/example.cfg`
Copying with Trivial File Transfer Protocol (TFTP)	`tftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: `tftp://172.1.1.1/example.cfg`
Copying with Secure Copy (SCP)	`scp://<username>@<location>[/<directory>][/<filename>]`	To specify a file in the configs directory on the server, logging on as user "bob": `e.g. scp://bob@10.10.0.12/configs/example.cfg`
Copying with SSH File Transfer Protocol (SFTP)	`sftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: `sftp://10.0.0.5/example.cfg`
Copying to or from stack member Flash	`<hostname>-<stack_ID>/flash:[/][<directory>/]<stack_member_filename>`	To specify a file in the configs directory on member 2 of a stack named vcstack: `vcstack-2/flash:/configs/example.cfg`

Valid characters

The URL can include characters from up to four categories. The URL categories are:

1. uppercase letters: A to Z
2. lowercase letters: a to z
3. digits: 0 to 9

4. special symbols: all printable ASCII characters not included in the previous three categories. Including the following characters:

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

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

Syntax for directory listings

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

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

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

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

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

In a stacked environment you can only access `flash` and `nvs` using the stack member filepath (e.g. `dir awplus-2/flash:/`). To access a USB storage device on a backup stack member, use the **remote-login** command on page 82.5.

Command List

autoboot enable

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

When the Autoboot feature is enabled, the device looks for a special file called `autoboot.txt` on the external media. If this file exists, the device will check the key and values in the file and recover the device with a new release file and/or configuration file from the external media. An example of a valid `autoboot.txt` file is shown in Figure 7-1 below.

Figure 7-1: Example autoboot.txt file

```
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=GS900-5.4.4E-1.1.rel
Boot_Config=network1.cfg
```

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

Note This command is not supported in a stacked configuration.

Syntax

```
autoboot enable
no autoboot enable
```

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

Mode Global Configuration

Example To enable the Autoboot feature, use the command:

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

To disable the Autoboot feature, use the command:

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

Related Commands

create autoboot
show autoboot
show boot

boot config-file

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

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

Syntax

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

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

Mode Global Configuration

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

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

For an explanation of the configuration fallback order, see **"The Configuration File Fallback Order" on page 6.10**.

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

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

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

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

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

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

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

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

Related Commands

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

boot config-file backup

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

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

Syntax

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

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

Mode Global Configuration

Usage For an explanation of the configuration fallback order, see **"The Configuration File Fallback Order" on page 6.10**.

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

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

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

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

Related Commands

boot config-file
boot system
boot system backup
show boot

boot system

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

```
% Stack member 2 has no card inserted
```

Examples To run the release file `GS900-5.4.4E-1.1.rel` stored on the switch's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/GS900-5.4.4E-1.1.rel
```

To remove the release file `GS900-5.4.4E-1.1.rel` stored on the switch's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system flash:/GS900-5.4.4E-1.1.rel
```

To run the release file `GS900-5.4.4E-1.1.rel` stored on the switch's USB storage device

filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system usb:/GS900-5.4.4E-1.1.rel
```

To remove the release file `GS900-5.4.4E-1.1.rel` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system usb:/GS900-5.4.4E-1.1.rel
```

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

```
awplus# configure terminal
awplus(config)# boot system GS900-5.4.4E-1.1.rel
```

```
Insufficient flash available on stack member-2 (11370496)
 to synchronize file GS900-5.4.4E-1.1.rel (14821895).

 List of release files on stack member-2
        GS900-5.4.4E-1.1.rel (14822400)

 Select files to free up space,
 Delete awplus-2/flash:/GS900-5.4.4E-1.1.rel? (y/n)[n]:y
```

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

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

Related Commands

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

boot system backup

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

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

Syntax

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

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

Mode Global Configuration

Examples To specify the file GS900-5.4.4E-1.1.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# boot system backup flash:/GS900-5.4.4E-1.1.rel
```

To remove the file GS900-5.4.4E-1.1.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system backup flash:/GS900-5.4.4E-
1.1.rel
```

Related Commands

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

cd

This command changes the current working directory.

Syntax `cd <directory-url>`

Parameter	Description
<directory-url>	URL of the directory.

Mode Privileged Exec

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

```
awplus# cd images
```

Related Commands
dir
pwd
show file systems

copy 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 USB when saving the software to the local filesystem.

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

Parameter	Description
<destination-url>	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. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

Related Commands
boot system backup
show boot

copy debug

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

Syntax

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

Parameter	Description
<destination-url>	The URL where you would like the debug output saved. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<source-url>	The URL where the debug output originates. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

```
awplus# copy debug usb:mydebug
```

Output **Figure 7-2: CLI prompt after entering the copy debug command**

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

Related Commands

delete debug
move debug

copy running-config

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

Syntax

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

Parameter	Description
<source-url>	The URL of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this when you want the script in the file to become the new running-config. The URL can contain the following protocols or location words. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<destination-url>	The URL where you would like the current running-config saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax. If you do not specify a file name, the switch saves the running-config to a file called default.cfg.
`startup-config`	Copies the running-config into the file set as the current startup-config file.

Mode Privileged Exec

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

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

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

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

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

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

Related Commands

copy startup-config
write file
write memory

copy startup-config

This command copies the startup-config script into a destination file, or alternatively copies a configuration script from a source file into the startup-config file. Specify whether the destination is Flash or USB when loading from the local filesystem.

Syntax

```
copy <source-url> startup-config
copy startup-config <destination-url>
```

Parameter	Description
<source-url>	The URL of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this to copy the script in the file into the *startup-config* file. Note that this does not make the copied file the new startup file, so any further changes made in the configuration file are not added to the startup-config file unless you reuse this command. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<destination-url>	The destination and filename that you are saving the startup-config as. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

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

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

Related Commands **copy running-config**

copy (URL)

This command copies a file. This allows you to:

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

Syntax `copy <source-url> <destination-url>`

Parameter	Description
<source-url>	The URL of the source file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<destination-url>	The URL for the destination file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

Usage The URL can include characters from up to four categories. The URL categories are:

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

copy zmodem
edit (URL)
show file systems

copy zmodem

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

Syntax

```
copy <source-url> zmodem
```

```
copy zmodem
```

Parameter	Description
<source-url>	The URL of the source file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

Related Commands

copy (URL)
show file systems

create autoboot

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

Syntax `create autoboot [usb]`

Mode Privileged Exec

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

```
awplus# create autoboot usb
```

Related Commands
autoboot enable
show autoboot
show boot

delete

This command deletes files or directories.

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

Parameter	Description
`force`	Ignore nonexistent filenames and never prompt before deletion.
`recursive`	Remove the contents of directories recursively.
<url>	URL of the file to delete. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

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

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

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

```
awplus# delete recursive old_configs
```

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

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

Related Commands **erase startup-config**
rmdir

delete debug

Use this command to delete a specified debug output file.

Syntax `delete debug <source-url>`

Parameter	Description
<source-url>	The URL where the debug output originates. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

Output **Figure 7-3: CLI prompt after entering the delete debug command**

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

Related Commands **copy debug**
move debug

dir

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

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

Parameter	Description
`all`	List all files.
`recursive`	List the contents of directories recursively.
`sort`	Sort directory listing.
`reverse`	Sort using reverse order.
`name`	Sort by name.
`size`	Sort by size.
`time`	Sort by modification time (default).
<url>	URL of the directory or file. If no directory or file is specified, then this command lists the files in the current working directory.
`debug`	Debug root directory
`flash`	Flash memory root directory
`nvs`	NVS memory root directory
`usb`	USB storage device root directory

Mode Privileged Exec

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

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

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

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

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

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

```
awplus# dir sort name
```

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

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

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

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

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

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

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

Related Commands

cd
pwd

edit

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

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

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

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

For more information about using the editor, including control sequences, see **"Using the Editor" on page 6.6**.

Syntax `edit [<filename>]`

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

Mode Privileged Exec

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

```
awplus# edit
```

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

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

Related Commands **edit (URL)**
show file

edit (URL)

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

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

Syntax `edit <url>`

Parameter	Description
<url>	The URL of the remote file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

Usage The URL can include characters from up to four categories. The URL categories are:

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

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

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

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

Related Commands
copy (URL)
edit
show file

erase startup-config

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

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

Syntax

```
erase startup-config
```

Mode

Privileged Exec

Example

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

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

Related Commands

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

mkdir

This command makes a new directory.

Syntax `mkdir <url>`

Parameter	Description
<url>	URL of the directory that you are creating.

Mode Privileged Exec

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

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

```
awplus# mkdir images
```

Related Commands **cd**
dir
pwd

move

This command renames or moves a file.

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

Parameter	Description
<source-url>	The URL of the source file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<destination-url>	The URL of the destination file. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

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

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

Related Commands
delete
edit
show file
show file systems

move debug

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

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

Syntax

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

Parameter	Description
<destination-url>	The URL where you would like the debug output moved to. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.
<source-url>	The URL where the debug output originates. See **"URL Syntax and Keyword Usage" on page 7.3** for valid URL syntax.

Mode Privileged Exec

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

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

Output **Figure 7-4: CLI prompt after entering the move debug command**

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

Related Commands

copy debug
delete debug

pwd

This command prints the current working directory.

Syntax `pwd`

Mode Privileged Exec

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

```
awplus# pwd
```

Related Commands cd

rmdir

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

Syntax `rmdir [force] <url>`

Parameter	Description
`force`	Optional keyword that allows you to delete any directories that are not empty and may contain files or subdirectories.
`<url>`	The URL of the directory.

Mode Privileged Exec

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

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

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

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

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

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

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

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

Related Commands
cd
dir
mkdir
pwd

show autoboot

This command displays the Autoboot configuration and status.

Syntax `show autoboot`

Mode Privileged Exec

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

```
awplus# show autoboot
```

Output **Figure 7-5: Example output from the show autoboot command**

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

Restore information on USB
Autoboot enable in autoboot.txt  : yes
Restore release file             : GS900-5.4.4E-1.1.rel (file exists)
Restore configuration file       : network_1.cfg (file exists)
```

Figure 7-6: Example output from the show autoboot command when an external media source is not present

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

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

show boot

This command displays the current boot configuration.

Syntax `show boot`

Mode Privileged Exec

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

```
awplus# show boot
```

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

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : usb:/GS900-5.4.4E.rel
Backup  boot image : flash:/GS900-5.4.4E.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

Figure 7-8: Example output from the show boot command

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : flash:/GS900-5.4.4E.rel
Backup  boot image : flash:/GS900-5.4.4E.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

Table 7-1: Parameters in the output of the show boot command

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

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

Related Commands

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

show file

This command displays the contents of a specified file.

Syntax `show file {<filename>|<url>}`

Parameter	Description
<filename>	Name of a file on the local Flash filesystem.
<url>	URL of a file.

Mode Privileged Exec

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

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

Related Commands **edit**
edit (URL)
show file systems

show file systems

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

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

Syntax `show file systems`

Mode Privileged Exec

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

```
awplus# show file systems
```

Output **Figure 7-9: Example output from the show file systems command**

```
awplus#show file systems
 Size(b)  Free(b)  Type   Flags  Prefixes   S/D/V   Lcl/Ntwk  Avail
-----------------------------------------------------------------
  63.0M    29.4M   flash     rw  flash:     static  local      Y
     -        -   system    rw  system:    virtual local      -
  10.0M     9.9M   debug     rw  debug:     static  local      Y
 499.0K   404.0K   nvs       rw  nvs:       static  local      Y
     -        -   usbstick  rw  usb:       dynamic local      N
     -        -   tftp      rw  tftp:      -       network    -
     -        -   scp       rw  scp:       -       network    -
     -        -   sftp      ro  sftp:      -       network    -
     -        -   http      ro  http:      -       network    -
     -        -   rsync     rw  rsync:     -       network    -
```

Table 7-2: Parameters in the output of the show file systems command

Parameter	Description
`Size (B) Available`	The total memory available to this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.
`Free (B)`	The total memory free within this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.
`Type`	The memory type used for this filesystem: flash, system, nvs, usbstick, tftp, scp, sftp, or http.
`Flags`	The file setting options: rw (read write), ro (read only).
`Prefixes`	The prefixes used when entering commands to access the filesystems: flash, system, nvs, usb, tftp, scp, sftp, or http.
`S/V/D`	The memory type: static, virtual, dynamic.
`Lcl / Ntwk`	Whether the memory is located locally or via a network connection.
`Avail`	Whether the memory is accessible: Y (yes), N (no), - (not appropriate)

Related Commands

edit
edit (URL)
show file

show running-config

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

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

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

For more information, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show running-config`

Mode Privileged Exec and Global Configuration

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

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

Output **Figure 7-10: Example output from the show running-config command**

```
GS900>ena
GS900#show running-config
!
service password-encryption
!
hostname GS900
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
platform hwfilter-size ipv4-limited-ipv6
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
snmp-server enable trap dhcpsnooping
!
aaa authentication enable default local
aaa authentication login default local
!
!
stack virtual-mac
stack virtual-chassis-id 746
!
ip domain-lookup
!
no service dhcp-server
!
spanning-tree mode rstp
!
auth-web-server gateway 192.168.1.1 vlan 1
latform l3-hashing-algorithm crc16l
!
mls qos enable
!
policy-map pmap1
 class default
!
switch 1 provision GS948MX
!
interface port1.0.1-1.0.26
 switchport
 switchport mode access
!
interface vlan1
 ip address 192.168.1.1/24
!
!
line con 0
line vty 0 4
!
end

GS900#
```

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

show running-config access-list

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config access-list
```

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-11: Example output from the show running-config access-list command

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

Related Commands

copy running-config
show running-config

show running-config as-path access-list

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

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

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-12: Example output from the show running-config as-path access-list command

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

Related Commands

copy running-config
show running-config

show running-config dhcp

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

Syntax `show running-config dhcp`

Mode Privileged Exec and Global Configuration

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

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

Output **Figure 7-13: Example output from the show running-config dhcp command**

```
!
#show running-config dhcp
no service dhcp-server
!
service dhcp-snooping
!
interface port1.0.1
 ip dhcp snooping trust
!
interface port1.0.3
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
!
interface port1.0.4
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
!
interface po1
 ip dhcp snooping max-bindings 25
 arp security violation log
!
interface sa1
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
 arp security violation log
!
interface vlan100
 ip dhcp snooping
 arp security
!
interface vlan200
 ip dhcp snooping
 arp security
!
```

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

show running-config full

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show running-config full`

Mode Privileged Exec and Global Configuration

Example To display the complete status and configuration of the running system, use the command:

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

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

show running-config interface

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show running-config interface [<interface-list>] [dot1x|ip igmp|lacp|mstp|rip|rstp|stp]`

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen, e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`dot1x`	Displays running configuration for 802.1X port authentication for the specified interfaces.
`lacp`	Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.
`ip igmp`	Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.
`ip multicast`	Displays running configuration for general multicast settings for the specified interfaces.
`mstp`	Displays running configuration for MSTP (Multiple Spanning Tree Protocol) for the specified interfaces.
`rip`	Displays running configuration for RIP (Routing Information Protocol) for the specified interfaces.
`rstp`	Displays running configuration for RSTP (Rapid Spanning Tree Protocol) for the specified interfaces.
`stp`	Displays running configuration for STP (Spanning Tree Protocol) for the specified interfaces.

Mode Privileged Exec and Global Configuration

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

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

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

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

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

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

Output **Figure 7-14: Example output from a show running-config interface port1.0.2 command**

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

Figure 7-15: Example output from the show running-config interface command

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

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

show running-config ip route

Use this command to show the running system static IPv4 route configuration.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config ip route
```

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-16: Example output from the show running-config ip route command

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

Related Commands

copy running-config
show running-config

show running-config ipv6 access-list

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

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

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-17: Example output from the show running-config ipv6 access-list command

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

Related Commands

copy running-config
show running-config

show running-config ipv6 route

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config ipv6 route
```

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-18: Example output from the show running-config ipv6 route command

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

Related Commands

copy running-config
show running-config

show running-config key chain

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config key chain
```

Mode

Privileged Exec and Global Configuration

Example

To display the running system key-chain related configuration, use the command:

```
awplus# show running-config key chain
```

Output

Figure 7-19: Example output from the show running-config key chain command

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

Related Commands

copy running-config
show running-config

show running-config lldp

This command shows the current running configuration of LLDP.

Syntax `show running-config lldp`

Mode Privileged Exec and Global Configuration

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

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

Output **Figure 7-20: Example output from the show running-config lldp command**

```
awplus#show running-config lldp

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

Related Commands **show lldp**
show lldp interface

show running-config power-inline

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

See **Chapter 22, Power over Ethernet Introduction** and **Chapter 23, Power over Ethernet Commands** for more information about PoE.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

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

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-21: Example output from the show running-config power-inline command

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

Related Commands

power-inline usage-threshold
show power-inline

show running-config route-map

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config route-map
```

Mode

Privileged Exec and Global Configuration

Example

To display the running system status and configuration details for route-map, use the command:

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

Output

Figure 7-22: Example output from the show running-config route-map command

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

Related Commands

copy running-config
show running-config

show running-config router

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show running-config router <protocol>`

Parameter	Description
`<protocol>`	rip or vrrp
`rip`	Routing Information Protocol (RIP)
`vrrp`	Virtual Redundancy Routing Protocol (VRRP)

Mode Privileged Exec and Global Configuration

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

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

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

show running-config router-id

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show running-config router-id
```

Mode

Privileged Exec and Global Configuration

Example

To display the running system global router ID configuration, use the command:

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

Output

Figure 7-23: Example output from the show running-config router-id command

```
!
router-id 3.3.3.3
!
```

Related Commands

copy running-config
show running-config

show running-config security-password

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

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

Mode

Privileged Exec and Global Configuration

Example

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

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

Output

Figure 7-24: Example output from the show running-config security-password command

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

Related Commands

show security-password configuration
show security-password user

show startup-config

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show startup-config`

Mode Privileged Exec

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

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

Output **Figure 7-25: Example output from the show startup-config command**

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

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

show version

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show version`

Mode User Exec and Privileged Exec

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

```
awplus# show version
```

Output **Figure 7-26: Example output from the show version command**

```
awplus#show version

AlliedWare Plus (TM) 5.4.3 19/11/12 13:22:32

Build name : GS900-5.4.4E-1.1.rel
Build date : Fri Jun 6 13:22:32 NZST 2014
Build type : RELEASE
 NET-SNMP SNMP agent software
   (c) 1996, 1998-2000 The Regents of the University of California.
       All rights reserved;
   (c) 2001-2003, Networks Associates Technology, Inc. All rights reserved.
   (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.
   (c) 2003, Sun Microsystems, Inc. All rights reserved.
   (c) 2003-2006, Sparta, Inc. All rights reserved.
   (c) 2004, Cisco, Inc and Information Network
       Center of Beijing University of Posts and Telecommunications.
       All rights reserved.
 RSA Data Security, Inc. MD5 Message-Digest Algorithm
   (c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
 OpenSSL Library
   Copyright (C) 1998-2011 The OpenSSL Project. All rights reserved.
 Original SSLeay License
   Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com).
 sFlow(R) Agent Software
   Copyright (c) 2002-2006 InMon Corp.
 DHCP Library
   Copyright (c) 2004-2012 by Internet Systems Consortium, Inc. ("ISC")
   Copyright (c) 1995-2003 by Internet Software Consortium.
 DHCP Bind
   Copyright (c) 2005 - 2008, Holger Zuleger HZnet. All rights reserved.
 Application Interface Specification Framework
   Copyright (c) 2002-2004 MontaVista Software, Inc;
   Copyright (c) 2005-2010 Red Hat, Inc.
 Hardware Platform Interface Library
   Copyright (c) 2004 by Intel Corp.
   Copyright (C) IBM Corp. 2004-2008.
 Corosync Cluster Engine
   Copyright (c) 2002-2004 MontaVista Software, Inc. All rights reserved.
   Copyright (c) 2005-2010 Red Hat, Inc. File Utility Library
   Copyright (c) Ian F. Darwin 1986-1987, 1989-1992, 1994-1995.
   Software written by Ian F. Darwin and others;
   maintained 1994- Christos Zoulas.
 ProL2TP
   Copyright Katalix Systems Ltd, 2010, 2011.
   All rights reserved.

Portions of this product are covered by the GNU GPL, source code may be
downloaded from: http://www.alliedtelesis.co.nz/support/gpl/awp.html
```

Related Commands **boot system backup**
show boot

write file

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

Syntax `write [file]`

Mode Privileged Exec

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

```
awplus# write file
```

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

write memory

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

Syntax `write [memory]`

Mode Privileged Exec

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

```
awplus# write memory
```

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

write terminal

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

Syntax `write terminal`

Mode Privileged Exec

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

```
awplus# write terminal
```

Related Commands **show running-config**

Chapter 8: System Configuration and Monitoring Commands

Command List 8.2
banner exec 8.2
banner login (system) 8.4
banner motd 8.5
clock set 8.6
clock summer-time date 8.7
clock summer-time recurring 8.9
clock timezone 8.11
ecofriendly led 8.12
ecofriendly lpi 8.13
findme 8.15
hostname 8.17
max-fib-routes 8.19
max-static-routes 8.20
no debug all 8.21
reboot 8.22
reload 8.23
show clock 8.24
show cpu 8.25
show cpu history 8.28
show debugging 8.30
show ecofriendly 8.31
show interface memory 8.33
show memory 8.35
show memory allocations 8.37
show memory history 8.38
show memory pools 8.40
show memory shared 8.41
show process 8.42
show reboot history 8.44
show router-id 8.45
show system 8.46
show system environment 8.47
show system interrupts 8.48
show system mac 8.49
show system pci device 8.50
show system pci tree 8.51
show system pluggable 8.52
show system pluggable detail 8.55
show system pluggable diagnostics 8.59
show system serialnumber 8.62
show tech-support 8.63
speed (asyn) 8.66
system territory (deprecated) 8.67
terminal monitor 8.68
undebug all 8.69

Command List

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

banner exec

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

Syntax

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

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

```
AlliedWare Plus (TM) Version 5.4.4E-1 03/31/14 00:44:25
```

Mode Global Configuration

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

```
awplus#configure terminal
awplus(config)#banner exec enable to move to Priv Exec mode
awplus(config)#exit
awplus#exit

awplus login: manager
Password:
enable to move to Priv Exec mode
awplus>
```

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

```
awplus#configure terminal
awplus(config)#banner exec default
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) Version 5.4.4E-1 03/31/14 13:03:59


awplus>
```

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

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

awplus login: manager
Password:
awplus>
```

Related Commands

banner login (system)
banner motd

banner login (system)

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

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

Syntax

```
banner login
no banner login
```

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

Mode Global Configuration

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

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

authorised users only
awplus login: manager
Password:

AlliedWare Plus (TM) Version 5.4.4E-1 03/31/14 13:03:59


awplus>
```

To remove the login banner, enter the following commands:

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

awplus login: manager
Password:

awplus>
```

Related Commands **banner exec**
banner motd

banner motd

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

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

Syntax

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

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

Mode Global Configuration

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

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

system shutdown at 6pm
awplus login: manager
Password:

AlliedWare Plus (TM) Version 5.4.4E-1 03/31/14 13:03:59
```

To remove the login banner, enter the following commands:

```
awplus>enable
awplus#configure terminal
awplus(config)#no banner motd
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) Version 5.4.4E-1 03/31/14 13:03:59


awplus>
```

Related Commands **banner exec**
banner login (system)

clock set

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

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

Parameter	Description
<hh:mm:ss>	Local time in 24-hour format
<day>	Day of the current month <1-31>
<month>	The first three letters of the current month.
<year>	Current year <2000-2035>

Mode Privileged Exec

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

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

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

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

Related Commands clock timezone

clock summer-time date

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

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates and recurring dates (set with the **clock summer-time recurring** command on page 8.9).

By default, the device has no summertime definitions set.

Syntax

```
clock summer-time <timezone-name> date <start-day> <start-month>
   <start-year> <start-time> <end-day> <end-month> <end-year>
   <end-time> <1-180>

no clock summer-time
```

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
date	Specifies that this is a date-based summertime setting for just the specified year.
<start-day>	Day that the summertime starts, in the range 1-31.
<start-month>	First three letters of the name of the month that the summertime starts.
<start-year>	Year that summertime starts, in the range 2000-2035.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-day>	Day that summertime ends, in the range 1-31.
<end-month>	First three letters of the name of the month that the summertime ends.
<end-year>	Year that summertime ends, in the range 2000-2035.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with the summertime set to begin on the 1st October 2007 and end on the 18th of March 2008:

```
awplus(config)# clock summer-time NZDT date 1 oct 2:00 2007 18
                mar 2:00 2008 60
```

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

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

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

clock summer-time recurring

This command defines the start and end of summertime for every year, and specifies summertime's offset value to Standard Time.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates (set with the **clock summer-time date** command on page 8.7) and recurring dates.

By default, the device has no summertime definitions set.

Syntax

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

no clock summer-time
```

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

Mode Global Configuration

Examples

To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with summertime set to start on the 1st Sunday in October, and end on the 3rd Sunday in March, use the command:

```
awplus(config)# clock summer-time NZDT recurring 1 sun oct 2:00
                3 sun mar 2:00 60
```

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

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

Related Commands

clock summer-time date
clock timezone

clock timezone

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

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

By default, the system time is set to UTC.

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related Commands

clock set
clock summer-time date
clock summer-time recurring

ecofriendly led

Use this command to enable the eco-friendly LED (Light Emitting Diode) feature, which turns off power to the port LEDs, including the stack port status LEDs. Power to the system status, SD and stack management LEDs is not disabled.

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

Syntax

```
ecofriendly led
no ecofriendly led
```

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

Mode Global Configuration

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

In a stack environment, enabling the eco-friendly LED feature on the stack master will apply the feature to every member of the stack.

For an example of how to configure a trigger to enable the eco-friendly LED feature, see **"Turn Off Power to Port LEDs" on page 75.7**. See also the section **"Save Power with the Eco-Friendly Feature" on page 1.32**.

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

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

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

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

Related Commands

ecofriendly lpi
show ecofriendly

ecofriendly lpi

Use this command to conserve power by enabling the eco-friendly LPI (Low Power Idle) feature. This feature reduces the power supplied to the ports by the switch whenever the ports are idle and are connected to IEEE 802.3az Energy Efficient Ethernet compliant host devices. See the section **"Save Power with the Eco-Friendly Feature" on page 1.32**.

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

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

Syntax

```
ecofriendly lpi
no ecofriendly lpi
```

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

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

Usage For an example of how to configure a trigger to enable the eco-friendly LPI feature, see **"Reduce Power Supplied to Ports" on page 75.9**.

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

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

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

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

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

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

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

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

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# no ecofriendly lpi
```

Related Commands

duplex
ecofriendly led
show ecofriendly
show interface
speed

findme

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

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

Syntax

```
findme [interface <port-list>|member <stack-ID>] [timeout <duration>]
no findme
```

Parameter	Description
<port-list>	The ports to flash. The port list can be: ■ a switch port, e.g. `port1.0.4` ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.5-1.0.6`.
<stack-ID>	Stack member number, from 1 to 4.
<duration>	Specify the duration in seconds within the range of 5-3600 seconds.

Default By default all port LEDs flash for 60 seconds.

Mode Privileged Exec

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

You can specify a particular stack member with the optional **member** parameter. All available interfaces are flashed by default.

Note The **interface** and **member** parameters are mutually exclusive.

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

```
awplus# findme
```

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

```
awplus# findme timeout 120
```

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

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

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

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

```
awplus# no findme
```

To activate the Find Me feature for the default duration on stack member 2, use the following command:

```
awplus# findme member 2
```

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

hostname

This command sets the name applied to the device as shown at the prompt. The hostname is:

- displayed in the output of the **show system** command
- displayed in the CLI prompt so you know which device you are configuring
- stored in the MIB object sysName

On a stack, after the stack master is elected, the master will have a host name: `awplus` by default, and this also becomes the name of the stack. Individual stack members (excluding the master) will have a host name that is the stack name hyphenated with a numeric suffix. For example, `awplus-1`, `awplus-2` and so on.

The hostname command can then be used to change the stack name and the stack master's host name. For example, for the hostname `Lab` the stack master's host name will be `Lab` and the other stack members will have host names `Lab-1`, `Lab-2` and so on.

In case of stack master fail-over, or stack split, the new stack will use the previous stack name as its host name and the stack name, unless it is changed by executing the hostname command on the new stack master.

Use the **no** variant of this command to revert the hostname setting to its default (`awplus`).

Syntax

```
hostname <hostname>
no hostname [<hostname>]
```

Parameter	Description
<hostname>	Specifies the name given to a specific switch. Also referred to as the Node Name in AMF output screens.

Default `awplus`

Mode Global Configuration

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

Note

Within an AMF network, any switch without a hostname applied will automatically be assigned a name based on its MAC address.

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

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

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

This changes the prompt to:

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

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

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

This changes the prompt to:

```
awplus(config)#
```

When AMF is configured, running the **no hostname** command will apply a hostname that is based on the MAC address of the switch node, for example, **node_0016_76b1_7a5e**.

Related Commands **show system**

max-fib-routes

This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds. The operation of these parameters is explained in the Parameter / Descriptions table shown below.

Note To set static routes, use the **max-static-routes** command on page 8.20.

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

Syntax

```
max-fib-routes <1-4294967294> [<1-100>|warning-only]

no max-fib-routes
```

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

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

Mode Global Configuration

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

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

max-static-routes

Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes. Note that FIB routes are set and reset using **max-fib-routes**.

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

Note To set dynamic FIB routes, use the **max-fib-routes** command on page 8.19.

Syntax

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

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

Mode Global Configuration

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

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

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

Related Commands **max-fib-routes**

no debug all

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

The debugging facility is disabled by default.

Syntax `no debug all [dot1x|ipv6|nsm]`

Parameter	Description
`dot1x`	Turns off all debugging for IEEE 802.1X port-based network access-control.
`ipv6`	Turns off all debugging for IPv6 (Internet Protocol version 6).
`nsm`	Turns off all debugging for the NSM (Network Services Module).

Mode Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

To disable all 802.1X debugging, use the command:

```
awplus# no debug all
```

To disable all IPv6 debugging, use the command:

```
awplus# no debug all
```

To disable all NSM debugging, use the command:

```
awplus# no debug all
```

Related Commands **undebug all**

reboot

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

You can reboot a stand-alone device, a stack, or a specified stack member.

Syntax

```
reboot <stack-ID>
reload <stack-ID>
reboot
reload
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Mode Privileged Exec

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

When restarting the whole stack, you can either use this reboot command to reboot all stack members immediately, or to minimize downtime, reboot the stack members in a rolling sequence by using the **reboot rolling** command on page 82.4.

Examples To restart the stand-alone device, use the command:

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

To restart all devices in the stack, use the command:

```
awplus# reboot
Are you sure you want to reboot the whole stack? (y/n): y
```

To restart stack member 2, use the command:

```
awplus# reboot stack-member 2
reboot stack-member 2 system? (y/n): y
```

If the specified stack member ID does not exist in the current stack, the command is rejected.

Related Commands

reboot rolling
reload rolling

reload

This command performs the same function as the **reboot** command on page 8.22.

show clock

This command displays the system's current configured local time and date. It also displays other clock related information such as timezone and summertime configuration.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show clock`

Mode User Exec and Privileged Exec

Example To display the system's current local time, use the command:

```
awplus# show clock
```

Output **Figure 8-1: Example output from the show clock command for a switch using New Zealand time**

```
Local Time: Mon,  6 Aug 2007 13:56:06 +1200
UTC Time:   Mon,  6 Aug 2007 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Table 8-1: Parameters in the output of the show clock command

Parameter	Description
`Local Time`	Current local time.
`UTC Time`	Current UTC time.
`Timezone`	The current configured timezone name.
`Timezone Offset`	Number of hours offset to UTC.
`Summer time zone`	The current configured summertime zone name.
`Summer time starts`	Date and time set as the start of summer time.
`Summer time ends`	Date and time set as the end of summer time.
`Summer time offset`	Number of minutes that summer time is offset from the system's timezone.
`Summer time recurring`	Whether the device will apply the summer time settings every year or only once.

Related Commands
clock set
clock summer-time date
clock summer-time recurring
clock timezone

show cpu

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show cpu [<stack-ID>] [sort {thrds|pri|sleep|runtime}]`

Parameter	Description	
<stack-ID>	Stack member number, from 1 to 4.	
sort	Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization.	
	thrds	Sort by the number of threads.
	pri	Sort by the process priority.
	sleep	Sort by the average time sleeping.
	runtime	Sort by the runtime of the process.

Mode User Exec and Privileged Exec

Usage Entering this command on the stack master will display the information for all the stack members. A stack member heading will distinguish the different information for every stack member device.

Examples To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```
awplus# show cpu sort thrds
```

Note that in a stack environment, executing this command on the stack master will show CPU utilization for all stack members.

To show CPU utilization for a specific stack member (in this case stack member 2), use the following command:

```
awplus# show cpu 2
```

Output **Figure 8-2: Example output from the show cpu command**

```
Stack member 2:

CPU averages:
 1 second: 12%, 20 seconds: 2%, 60 seconds: 2%
System load averages:
 1 minute: 0.03, 5 minutes: 0.02, 15 minutes: 0.00
Current CPU load:
 userspace: 6%, kernel: 4%, interrupts: 1% iowaits: 0%

user processes
==============
  pid name             thrds  cpu%   pri state sleep% runtime
 1544 hostd               1   2.8    20   run      0   120
 1166 exfx               17   1.8    20 sleep      0  3846
 1198 stackd              1   0.9    20 sleep      0   459
 1284 aisexec            44   0.9    -2 sleep      0  2606
    1 init                1   0.0    20 sleep      0   120
 9772 sh                  1   0.0    20 sleep      0     0
 9773 corerotate          1   0.0    20 sleep      0     0
  853 syslog-ng           1   0.0    20 sleep      0   356
  859 klogd               1   0.0    20 sleep      0     1
  910 inetd               1   0.0    20 sleep      0     3
  920 portmap             1   0.0    20 sleep      0     0
  931 crond               1   0.0    20 sleep      0     1
 1090 openhpid           11   0.0    20 sleep      0   233
 1111 hpilogd             1   0.0    20 sleep      0     0
 1240 hsl                 1   0.0    20 sleep      0    79
 1453 authd               1   0.0    20 sleep      0    85
 1497 cntrd               1   0.0    20 sleep      0     2
 1520 epsrd               1   0.0    20 sleep      0    56
 1571 imi                 1   0.0    20 sleep      0   275
 1594 irdpd               1   0.0    20 sleep      0    23
 1617 lacpd               1   0.0    20 sleep      0    87
 1638 mstpd               1   0.0    20 sleep      0    75
 1662 nsm                 1   0.0    20 sleep      0   163
 1685 ospfd               1   0.0    20 sleep      0    35
 1708 pdmd                1   0.0    20 sleep      0    23
 1729 pimd                1   0.0    20 sleep      0    32
 1751 ripd                1   0.0    20 sleep      0    33
 1775 ripngd              1   0.0    20 sleep      0    25
 1797 rmond               1   0.0    20 sleep      0    64
 1963 ntpd                1   0.0    20 sleep      0    15
 2102 atlgetty            1   0.0    20 sleep      0     0
 2712 rpc.statd           1   0.0    20 sleep      0     0
 2716 rpc.statd           1   0.0    20 sleep      0     0
 2722 rpc.mountd          1   0.0    20 sleep      0     0
 2821 automount           1   0.0    20 sleep      0    82
 2892 ntpd                1   0.0    20 sleep      0    17
 2912 sshd                1   0.0    20 sleep      0     0
 9774 login               1   0.0    20 sleep      0     2
12689 more                1   0.0    20 sleep      0     0

.
.
.
```

Table 8-2: Parameters in the output of the show cpu command

Parameter	Description
`Stack member`	Stack member number.
`CPU averages`	Average CPU utilization for the periods stated.
`System load averages`	The average number of processes waiting for CPU time for the periods stated.
`Current CPU load`	Current CPU utilization specified by load types.

Table 8-2: Parameters in the output of the show cpu command (cont.)

Parameter	Description
`pid`	Identifier number of the process.
`name`	A shortened name for the process
`thrds`	Number of threads in the process.
`cpu%`	Percentage of CPU utilization that this process is consuming.
`pri`	Process priority state.
`state`	Process state; one of “run”, “sleep”, “zombie”, and “dead”.
`sleep%`	Percentage of time that the process is in the sleep state.
`runtime`	The time that the process has been running for, measured in jiffies. A jiffy is the duration of one tick of the system timer interrupt.

Related Commands

show memory
show memory allocations
show memory history
show memory pools
show process

show cpu history

This command prints a graph showing the historical CPU utilization.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show [<stack-ID>]cpu history`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Mode User Exec and Privileged Exec

Usage This command's output displays three graphs of the percentage CPU utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

If this command is entered on the stack master, it will print graphs for all the stack members. A stack member heading will be displayed to distinguish the different graphs for every stack member.

Examples To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

To display the CPU utilization history graph for stack member 2, use the command:

```
awplus# show 2 cpu history
```

where 2 is the node id of the stack member.

Output **Figure 8-3: Example output from the show cpu history command**

```
Stack member 2:

Per second CPU load history

100
 90
 80
 70
 60
 50
 40
 30
 20
 10 ************************************************************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                  Newest
        CPU load% per second (last 60 seconds)
              * = average CPU load%


Per minute CPU load history

100        *+
 90        +
 80
 70
 60
 50
 40
 30
 20                    +                   +
 10         ************************************************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                  Newest
        CPU load% per minute (last 60 minutes)
              * = average CPU load%, + = maximum


Per (30) minute CPU load history

100                                                            +
 90
 80
 70
 60
 50
 40
 30
 20
 10                                                           **
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                  Newest
        CPU load% per 30 minutes (last 60 values / 30 hours)
              * = average, - = minimum, + = maximum
.
.
.
```

Related Commands

show memory
show memory allocations
show memory pools
show process

show debugging

This command displays information for all debugging options.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging`

Default This command runs all the **show debugging** commands in alphabetical order.

Mode User Exec and Privileged Exec

Usage This command displays all debugging information, similar to the way the **show tech-support** command displays all show output for use by Allied Telesis authorized service personnel only.

Example To display all debugging information, use the command:

```
awplus# show debugging
```

Output **Figure 8-4: Example output from the show debugging command**

```
awplus#show debugging
AAA debugging status:
  Authentication debugging is off
  Accounting debugging is off
% DHCP Snooping service is disabled

802.1X debugging status:

EPSR debugging status:
 EPSR Info debugging is off
 EPSR Message debugging is off
 EPSR Packet debugging is off
 EPSR State debugging is off
IGMP Debugging status:
  IGMP Decoder debugging is off
  IGMP Encoder debugging is off
.
.
.
```

Related Commands

show debugging aaa
show debugging dot1x
show debugging epsr
show debugging igmp
show debugging lacp
show debugging lldp
show debugging mstp
show debugging power-inline
show debugging radius
show debugging snmp

show ecofriendly

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

Syntax `show ecofriendly`

Mode Privileged Exec and Global Configuration

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

```
awplus# show ecofriendly
```

Output **Figure 8-5: Example output from the show ecofriendly command**

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

Table 8-3: Parameters in the output of the show ecofriendly command

Parameter	Description
`normal`	The eco-friendly LED feature is disabled and port LEDs show the current state of the ports. This is the default setting.
`off`	The eco-friendly LED feature is enabled and power to the port LEDs is disabled.
`normal (configuration overridden by eco button)`	The eco-friendly LED feature has been disabled with the eco-switch button, overriding the configuration set with the **ecofriendly led** command. The port LEDs show the current state of the ports.
`off (configuration overridden by eco button)`	The eco-friendly LED feature has been enabled with the eco-switch button, overriding the configuration set with the **ecofriendly led** command. Power to the port LEDs is disabled.
`Port`	Displays the port number as assigned by the switch.
`Name`	Displays the port name if a name is configured for a port number.

Table 8-3: Parameters in the output of the show ecofriendly command (cont.)

Parameter	Description
`Configured`	The eco-friendly LPI feature is configured on the port. Either LPI or off is displayed.
`Status`	The eco-friendly LPI feature is active on the port. Either LPI or off is displayed. Ports that are not running show a dash (-).

Related Commands

ecofriendly led
ecofriendly lpi

show interface memory

This command displays the shared memory used by either all interfaces, or the specified interface or interfaces. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show interface memory
show interface <port-list> memory
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: ■ a switch port (e.g. `port1.0.4`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Mode User Exec and Privileged Exec

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

```
awplus# show interface memory
```

To display the shared memory used by `port1.0.1` and `port1.0.5 to port1.0.6`, use the command:

```
awplus# show interface port1.0.1,port1.0.5-1.0.6 memory
```

Output

Figure 8-6: Example output from the show interface <*port-list*> memory command

```
awplus#show interface port1.0.1,port1.0.5-1.0.6 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    393228       512            1
port1.0.5    491535       512            1
port1.0.6    557073       512            1
```

Figure 8-7: Example output from the show interface memory command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    393228       512            1
port1.0.2    458766       512            1
port1.0.3    360459       512            1
port1.0.4    524304       512            1
port1.0.5    491535       512            1
port1.0.6    557073       512            1
port1.0.7    327690       512            1
port1.0.8    655380       512            1
port1.0.9    622611       512            1
.
.
port1.0.21   950301       512            1
port1.0.22   1048608      512            1
port1.0.23   1015839      512            1
port1.0.24   1081377      512            1
lo           425997       512            1
po1          1179684      512            1
po2          1212453      512            1
sa3          1245222      512            1
```

Related Commands

show interface brief
show interface status

show memory

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show memory [<stack-ID>] [sort {size|peak|stk}]`

Parameter	Description	
`<stack-ID>`	Stack member number, from 1 to 4.	
`sort`	Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.	
	`size`	Sort by the amount of memory the process is currently using.
	`peak`	Sort by the amount of memory the process is currently using.
	`stk`	Sort by the stack size of the process.

Mode User Exec and Privileged Exec

Usage If this command is entered on the stack master, it will display corresponding memory utilization information for all the stack members. A stack member heading will display the information for every stack member device.

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

```
awplus# show memory
```

Output **Figure 8-8: Example output from the show memory command**

```
awplus#show memory

Stack member 1:

RAM total: 514920 kB; free: 382716; buffers: 16368 kB

user processes
==============
pid name            mem%   size   peak   data   stk
962 pss                6  33112  36260  27696   244
1   init               0    348   1092    288    84
797 syslog-ng          0    816   2152    752    84
803 klogd              0    184   1244    124    84
843 inetd              0    256   1256    136    84
.
.
.
```

Table 8-4: Parameters in the output of the show memory command

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

Related Commands

show memory allocations
show memory history
show memory pools
show memory shared

show memory allocations

This command displays the memory allocations used by processes.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show memory allocations [<process>]`

Parameter	Description
<process>	Displays the memory allocation used by the specified process.

Mode User Exec and Privileged Exec

Example To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

Output **Figure 8-9: Example output from the show memory allocations command**

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

Current 15093760 (peak 15093760)

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

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

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

Related Commands

show memory
show memory history
show memory pools
show memory shared
show tech-support

show memory history

This command prints a graph showing the historical memory usage.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show memory history <stack-ID>`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Mode User Exec and Privileged Exec

Usage This command's output displays three graphs of the percentage memory utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

If entered on the stack master, this command will display corresponding memory utilization information for all the stack members. A stack member heading will be displayed to distinguish the different lists for every stack member.

Examples To show a graph displaying the historical memory usage for either a single unstacked device, or a complete stack, use the command:

```
awplus# show memory history
```

To show a graph displaying the historical memory usage for specific stack member (stack member 2 in this example) within a stack, use the command:

```
awplus# show memory history 2
```

Output **Figure 8-10: Example output from the show memory history command**

```
STACK member 1:

Per minute memory utilization history

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

STACK member 2:

Per minute memory utilization history

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

Related Commands

show memory allocations
show memory pools
show memory shared
show tech-support

show memory pools

This command shows the memory pools used by processes.

For information on output options, see "Controlling "show" Command Output" on page 1.35.

Syntax `show memory pools [<process>]`

Parameter	Description
<process>	Displays the memory pools used by the specified process.

Mode User Exec and Privileged Exec

Example To shows the memory pools used by processes, use the command:

```
awplus# show memory pools
```

Output **Figure 8-11: Example output from the show memory pools command**

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

Current 15290368 (peak 15290368)

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

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

Related Commands
show memory allocations
show memory history
show tech-support

show memory shared

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show memory shared`

Mode User Exec and Privileged Exec

Example To display information about the shared memory allocation used on the switch, use the command:

```
awplus# show memory shared
```

Output **Figure 8-12: Example output from the show memory shared command**

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

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

Related Commands
show memory allocations
show memory history
show memory sort

show process

This command lists a summary of the current running processes.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show process [<stack-ID>] [sort {cpu|mem}]`

Parameter	Description	
<stack-ID>	Stack member number, from 1 to 4.	
sort	Changes the sorting order for the list of processes.	
	cpu	Sorts the list by the percentage of CPU utilization.
	mem	Sorts the list by the percentage of memory utilization.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

Example To display a summary of the current running processes, use the command:

```
awplus# show process
```

To display a summary of the current running processes on stack member 2, use the command:

```
awplus# show process 2
```

Output **Figure 8-13: Example output from the show process command**

```
Stack member 2:

CPU load for 1 minute: 0%; 5 minutes: 3%; 15 minutes: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
==============
pid name          thrds  cpu%  mem%   pri  state  sleep%
962 pss             12     0     6    25  sleep       5
1   init             1     0     0    25  sleep       0
797 syslog-ng        1     0     0    16  sleep      88


kernel threads
==============
pid name          cpu%  pri  state  sleep%
71  aio/0         0     20   sleep  0
3   events/0      0     10   sleep  98
.
.
.
```

Table 8-5: Parameters in the output from the show process command

Parameter	Description
`Stack member`	Stack member number.
`CPU load`	Average CPU load for the given period.
`RAM total`	Total memory size.
`free`	Available memory.
`buffers`	Memory allocated to kernel buffers.
`pid`	Identifier for the process.
`name`	Short name to describe the process.
`thrds`	Number of threads in the process.
`cpu%`	Percentage of CPU utilization that this process is consuming.
`mem%`	Percentage of memory utilization that this process is consuming.
`pri`	Process priority.
`state`	Process state; one of “run”, “sleep”, “stop”, “zombie”, or “dead”.
`sleep%`	Percentage of time the process is in the sleep state.

Related Commands

show cpu
show cpu history

show reboot history

Use this command to display the switch's reboot history.

Syntax `show reboot history [<stack-ID>]`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Mode User Exec and Privileged Exec

Example To show the reboot history of stack member 2, use the command:

```
awplus# show reboot history 2
```

Output **Figure 8-14: Example output from the show reboot history command**

```
awplus#show reboot history 2

Stack member 2:

<date>     <time>    <type>      <description>
------------------------
2014-01-10 01:42:04  Expected    User Request
2014-01-10 01:35:31  Expected    User Request
2014-01-10 01:16:25  Unexpected Rebooting due to critical process (network/nsm)
failure!
2014-01-10 01:11:04  Unexpected Rebooting due to critical process (network/nsm)
failure!
2014-01-09 20:46:40  Unexpected Rebooting due to VCS duplicate member-ID
2014-01-09 19:56:16  Expected    User Request
2014-01-09 19:51:20  Expected    User Request
```

Table 8-6: Parameters in the output from the show reboot history command

Parameter	Description
`user request`	User initiated reboot via the CLI.

Related Commands show tech-support

show router-id

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show router-id`

Mode User Exec and Privileged Exec

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

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

Output **Figure 8-15: Example output from the show router-id command**

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

show system

This command displays general system information about the device, including the hardware installed, memory, and software versions loaded. It also displays location and contact details when these have been set.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system`

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

Output **Figure 8-16: Example output from the show system command**

```
GS900#show system
Stack System Status                                    Thu May 29 02:40:53 2014

Stack member 1

Board       ID  Bay   Board Name                          Rev   Serial number
-------------------------------------------------------------------------------
Base       392        GS948MX                             X1-0  A04939H131100021
-------------------------------------------------------------------------------
RAM:  Total: 494848 kB Free: 396052 kB
Flash: 62.0MB Used: 45.4MB Available: 16.6MB
-------------------------------------------------------------------------------
Environment Status : Normal
Uptime             : 0 days 00:40:53
Bootloader version : 3.0.3


Current software   : GS900-5.4.4E-1.1.rel
Software version   : 5.4.4E-0.1
Build date         : Thu May 29 01:32:39 NZST 2015

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

System Name
 GS900
System Contact

System Location

GS900#
```

Related Commands **show system environment**

show system environment

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

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system environment`

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

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

```
awplus# show system environment
```

Output **Figure 8-17: Example output from the show system environment command**

```
Stack Environment Monitoring Status

Stack member 1:

Overall Status: Normal

Resource ID: 1  Name: GS948MX
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Fan: Fan 1 (Rpm)                       4344       3000          -      Ok
2   Voltage: 1.8V (Volts)                 1.804      1.617      1.978     Ok
3   Voltage: 1.0V (Volts)                 0.995      0.896      1.099     Ok
4   Voltage: 3.3V (Volts)                 3.291      2.960      3.613     Ok
5   Voltage: 5.0V (Volts)                 5.066      4.477      5.498     Ok
6   Voltage: 1.2V (Volts)                 1.187      1.072      1.318     Ok
7   Temp: CPU (Degrees C)                    50        -10         90     Ok
```

Related Commands **show system**

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.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system interrupts`

Mode User Exec and Privileged Exec

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

```
awplus# show system interrupts
```

Output **Figure 8-18: Example output from the show system interrupts command**

```
awplus#show system interrupts
           CPU0
  5:   10428098 Enabled     0           MIPS  linux-kernel-bde
  6:          0 Enabled     0           MIPS  bcma-usb-ohci:usb1, bcma-usb-ehci:
usb2
  7:  300725368 Enabled     0           MIPS  timer
 18:  598364339 Enabled     0        MIPS-CC  bcma_i2c
 22:       4909 Enabled     0        MIPS-CC  serial
 31:          1 Enabled     0      MIPS-GPIO  GPIO-Ethernet PHY
 35:          2 Enabled     0      MIPS-GPIO  GPIO-ECO Button
 40:          4 Enabled     0      MIPS-GPIO  PSU Interrupt
 42:          0 Enabled     0      MIPS-GPIO  PSU2 power good
 43:          0 Enabled     0      MIPS-GPIO  PSU1 power good

ERR:          0
awplus#
```

Related Commands **show system environment**

show system mac

This command displays the physical MAC address available on a standalone switch, or a stack. This command also shows the virtual MAC address for a for a stack if the stack virtual MAC address feature is enabled with the **stack virtual-mac** or the **stack enable** command.

Syntax `show system mac`

Mode User Exec and Privileged Exec

Usage This command also displays the virtual MAC address, if the VCStack Plus virtual MAC address feature is enabled with the **stack virtual-mac** command.

For information about this VCStack Plus feature, see the section **Fixed or Virtual MAC Addressing** in the **VCStack Introduction** chapter.

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

```
awplus# show system mac
```

Output **Figure 8-19: Example output from the show system mac command**

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

Output **Figure 8-20: Example output showing how to use the stack virtual-mac command and the show system mac command**

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#stack virtual-mac
% Please check that the new MAC 0000.cd37.0065 is unique within
the network.
% Save the config and restart the system for this change to take
effect.
Member1#copy run start
Building configuration...
[OK]
Member1#reload
reboot system? (y/n): y

        ... Rebooting at user request ...
Loading default configuration
....

awplus login: manager
Password:

awplus>show system mac
eccd.6d9d.4eed

Virtual MAC Address 0000.cd37.0065
```

Related Commands **stack virtual-mac**

show system pci device

Use this command to display the PCI devices on your switch.

For information on output options, see "Controlling "show" Command Output" on page 1.35.

Syntax `show system pci device`

Mode User Exec and Privileged Exec

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

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

Output **Example output from the show system pci device command**

```
awplus#show system pci device
00:0c.0 Class 0200: 11ab:00d1 (rev 01)
        Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 113
        Memory at 5ffff000 (32-bit, non-prefetchable) [size=4K]
        Memory at 58000000 (32-bit, non-prefetchable) [size=64M]

00:0d.0 Class 0200: 11ab:00d1 (rev 01)
        Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 116
        Memory at 57fff000 (32-bit, non-prefetchable) [size=4K]
        Memory at 50000000 (32-bit, non-prefetchable) [size=64M]
```

```
Member1#show system pci device
00:00.0 Class 0600: 14e4:5300 (rev 01)
        Subsystem: 14e4:5300
        Flags: bus master, fast devsel, latency 0, IRQ 5
        Memory at 18000000 (64-bit, non-prefetchable) [size=16K]
        Memory at <unassigned> (64-bit, non-prefetchable) [size=128M]
        Capabilities: [40] Power Management version 3
        Capabilities: [58] #09 [0078]
        Capabilities: [48] Message Signalled Interrupts: 64bit+ Queue=0/0 Enable
-
        Capabilities: [d0] #10 [0041]

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

Member1#
```

Related Commands **show system environment**
show system pci tree

show system pci tree

Use this command to display the PCI tree on your switch.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show system pci tree
```

Mode

User Exec and Privileged Exec

Example

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

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

Output

Figure 8-21: Example output from the show system pci tree command

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

Related Commands

show system environment
show system pci device

show system pluggable

This command displays **brief** pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the switch. Different types of pluggable transceivers are supported in different models of switch. See your Allied Telesis dealer for more information about the models of pluggables that your switch supports.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system pluggable [<port-list>]`

Parameter	Description
<port-list>	The ports to display information about. The port list can be: ■ a switch port (e.g. `port1.0.12`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage Entering this command will display the information for all pluggable transceivers in the system. In a stack, a separate heading will be displayed to distinguish each stack member's information.

Example To display brief information about pluggable transceivers installed in `port1.0.1` through `port1.0.4`, use the command:

```
awplus# show system pluggable port1.0.1-1.0.4
```

Output **Figure 8-22: Example output from the show system pluggable port1.0.1-1.0.4 command**

```
System Pluggable Information
Port   Manufacturer     Device           Serial Number    Datecode Type
-------------------------------------------------------------------------------
1.0.1  AGILENT          HFBR-5710L       0401312315461272 040131   1000BASE-SX
1.0.2  AGILENT          QBCU-5730R       AK0614GKF7       060408   1000BASE-T
1.0.3  AGILENT          HFBR-5710L       0305130112182696 030513   1000BASE-SX
1.0.4  AGILENT          HBCU-5710R       AK051300SM       050402   1000BASE-T
-------------------------------------------------------------------------------
```

Example To display information about the pluggable transceiver installed in `port1.0.1`, use the command:

```
awplus# show system pluggable port1.0.1
```

Output **Figure 8-23: Example output from the show system pluggable port1.0.1 command**

```
System Pluggable Information
Port   Manufacturer     Device           Serial Number    Datecode Type
-------------------------------------------------------------------------------
1.0.1  AGILENT          HFBR-5710L       0401312315461272 040131   1000BASE-SX
-------------------------------------------------------------------------------
```

Table 8-7: Parameters in the output from the show system pluggables command

Parameter	Description
`Stack member`	The stack member number.
`Port`	Specifies the vendor's name for the installed pluggable transceiver.
`Vendor Name`	Specifies the vendor's name for the installed pluggable transceiver.
`Device Name`	Specifies the device name for the installed pluggable transceiver.
`Device Type`	Specifies the device type for the installed pluggable transceiver.
`Serial Number`	Specifies the serial number for the installed pluggable transceiver.
`Manufacturing Datecode`	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. See the **Trouble-shoot Fiber and Pluggable Issues** section in the **System Configuration and Monitoring Commands** chapter.
`SFP Laser Wavelength`	Specifies the laser wavelength of the installed pluggable transceiver.
`Datecode`	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. See the **Trouble-shoot Fiber and Pluggable Issues** section in the **System Configuration and Monitoring Commands** chapter.
`Device Type`	Specifies the device type for the installed pluggable transceiver

Related Commands

show system environment
show system pluggable detail
show system pluggable diagnostics

show system pluggable detail

This command displays detailed pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the switch. Different types of pluggable transceivers are supported in different models of switch. See your Allied Telesis dealer for more information about the models of pluggables that your switch supports.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system pluggable [<port-list>] detail`

Parameter	Description
<port-list>	The ports to display information about. The port list can be: ■ a switch port (e.g. `port1.0.12`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display detailed information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish the different pluggable transceiver information for every stack member.

In addition to the information about pluggable transceivers displayed using the **show system pluggable** command (port, manufacturer, serial number, manufacturing datecode, and type information), the **show system pluggable detail** command displays the following information:

- **SFP Laser Wavelength**: Specifies the laser wavelength of the installed pluggable transceiver
- **Single mode Fiber**: Specifies the link length supported by the pluggable transceiver using single mode fiber
- **OM1 (62.5µm) Fiber**: Specifies the link length (in µm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
- **OM2 (50 µm) Fiber**: Specifies the link length (in µm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
- **Diagnostic Calibration**: Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration.
  - « **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.
  - « **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration.
  - « - is displayed if SFP or SFP+ DDM Internal Calibration or External Calibration is not supported.
- **Power Monitoring**: Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in µW.

Note For parameters that are not supported or not specified, a hyphen is displayed instead.

Example To display detailed information about the pluggable transceivers installed in a particular port on the switch, use a command like:

```
awplus# show system pluggable port1.0.24 detail
```

To display detailed information about all the pluggable transceivers installed on the switch, use the command:

```
awplus# show system pluggable detail
```

Output **Figure 8-24: Example output from the show system pluggable detail command on a switch**

```
awplus#show system pluggable port1.0.24 detail
System Pluggable Information Detail

Port1.0.24
==========
Vendor Name:               AGILENT
Device Name:               HFCT-5710L
Device Type:               1000BASE-LX
Serial Number:             0402142241184360
Manufacturing Datecode:    040214
SFP Laser Wavelength:      -
Link Length Supported
 Single Mode Fiber :      10Km
 OM1 (62.5um) Fiber:      550m
 OM2 (50um) Fiber  :      550m
Diagnostic Calibration:    Internal
Power Monitoring:          Avg
FEC BER support:           -
```

Example To display detailed information about the pluggable transceivers installed on a stack, use the command:

```
awplus# show system pluggable detail
```

Output

Figure 8-25: Example output from the show system pluggable detail command on a stack

```
awplus#show system pluggable detail
System Pluggable Information Detail

Stack member 1:

Port1.0.24
==========
Vendor Name:               AGILENT
Device Name:               HFCT-5710L
Device Type:               1000BASE-LX
Serial Number:             0402142241184360
Manufacturing Datecode:    040214
SFP Laser Wavelength:      -
Link Length Supported
 Single Mode Fiber :      10Km
 OM1 (62.5um) Fiber:      550m
 OM2 (50um) Fiber  :      550m
Diagnostic Calibration:    Internal
Power Monitoring:          Avg
FEC BER support:           -

Stack member 2:

Port2.0.24
==========
Vendor Name:               FINISAR CORP.
Device Name:               FTRJ-8519-7D-CSC
Device Type:               1000BASE-SX
Serial Number:             P430KGY
Manufacturing Datecode:    030718
SFP Laser Wavelength:      850nm
Link Length Supported
  Single Mode Fiber :      -
  OM1 (62.5um) Fiber:      300m
  OM2 (50um) Fiber  :      550m
Diagnostic Calibration:    Internal
Power Monitoring:          OMA
FEC BER support:           Yes
```

Table 8-8: Parameters in the output from the show system pluggables detail command:

Parameter	Description
`Stack member`	The stack member number..
`Port`	Specifies the port the pluggable transceiver is installed in.
`Vendor Name`	Specifies the vendor's name for the installed pluggable transceiver.
`Device Name`	Specifies the device name for the installed pluggable transceiver.
`Device Type`	Specifies the device type for the installed pluggable transceiver..
`Serial Number`	Specifies the serial number for the installed pluggable transceiver.
`Manufacturing Datecode`	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. See the **Trouble-shoot Fiber and Pluggable Issues** section in the **System Configuration and Monitoring Commands** chapter.

Parameter	Description
`SFP Laser Wavelength`	Specifies the laser wavelength of the installed pluggable transceiver.
`Single Mode Fiber`	Specifies the link length supported by the pluggable transceiver using single mode fiber.
`OM1 (62.5um) Fiber`	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
`OM2 (50um) Fiber`	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
`Diagnostic Calibration`	Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration: **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration. **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration. - is displayed if SFP or SFP+ DDM Internal Calibration or External Calibration is not supported.
`Power Monitoring`	Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in µW.

Related Commands

show system environment
show system pluggable
show system pluggable diagnostics

show system pluggable diagnostics

This command displays diagnostic information about SFP and SFP+ pluggable transceivers, which support Digital Diagnostic Monitoring (DDM).

Different types of pluggable transceivers are supported in different models of switch. See your switch's Datasheet for more information about the models of pluggables that your switch supports.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system pluggable [<port-list>] diagnostics`

Parameter	Description
<port-list>	The ports to display information about. The port list can be: ■ a switch port (e.g. `port1.0.12`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish different pluggable transceiver information for every stack member.

Modern optical SFP and SFP+ transceivers support Digital Diagnostics Monitoring (DDM) functions.

Diagnostic monitoring features allow you to monitor real-time parameters of the pluggable transceiver, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. Additionally, RX LOS (Loss of Signal) is shown when the received optical level is below a preset threshold. Monitor these parameters to check on the health of all transceivers, selected transceivers or a specific transceiver installed in a switch.

Examples To display detailed information about all pluggable transceivers installed on a standalone switch, use the command:

```
awplus# show system pluggable diagnostics
```

Output **Figure 8-26: Example output from the show system pluggable diagnostics command**

```
awplus#show system pluggable diagnostics
System Pluggable Information Diagnostics

Port1.0.21            Status              Alarms                    Warnings
                    Reading   Alarm     Max     Min   Warning     Max     Min
Temp: (Degrees C)    29.387       -  100.00  -40.00         -  85.000  -10.00
Vcc: (Volts)          3.339       -   3.465   3.135         -   3.400   3.200
Tx Bias: (mA)        10.192       -  37.020   3.260         -  34.520   5.760
Tx Power: (mW)       17.872       -  35.643   8.953         -  28.313  11.271
Rx Power: (mW)        0.006     Low  15.849   0.025       Low  12.589   0.040
Rx LOS:              Rx Down

Port1.0.22            Status              Alarms                    Warnings
                    Reading   Alarm     Max     Min   Warning     Max     Min
Temp: (Degrees C)    29.387       -  100.00  -40.00         -  85.000  -10.00
Vcc: (Volts)          3.378       -   3.630   2.970         -   3.465   3.135
Tx Bias: (mA)         2.802       -   6.000   1.000         -   5.000   1.000
Tx Power: (mW)        2.900       -  11.000   0.600         -  10.000   0.850
Rx Power: (mW)        1.739       -  18.000   0.000         -  10.000   0.200
Rx LOS:               Rx Up
```

To display detailed information about the pluggable transceiver installed in `port1.0.22` on a standalone switch, use the command:

```
awplus# show system pluggable diagnostics port1.0.22
```

Output **Figure 8-27: Example output from the show system pluggable diagnostics port1.0.22 command**

```
awplus#show system pluggable port1.0.22 diagnostics
System Pluggable Information Diagnostics

Port1.0.22            Status              Alarms                    Warnings
                    Reading   Alarm     Max     Min   Warning     Max      Min
Temp: (Degrees C)    29.387       -  100.00  -40.00         -  85.000   -10.00
Vcc: (Volts)          3.378       -   3.630   2.970         -   3.465    3.135
Tx Bias: (mA)         2.802       -   6.000   1.000         -   5.000    1.000
Tx Power: (mW)        2.900       -  11.000   0.600         -  10.000    0.850
Rx Power: (mW)        1.739       -  18.000   0.000         -  10.000    0.200
Rx LOS:               Rx Up
```

Table 8-9: Parameters in the output from the show system pluggables diagnostics command

Parameter	Description
`Temp (Degrees C)`	Shows the temperature inside the transceiver.
`Vcc (Volts)`	Shows voltage supplied to the transceiver.
`Tx Bias (mA)`	Shows current to the Laser Diode in the transceiver.
`Tx Power (mW)`	Shows the amount of light transmitted from the transceiver.
`Rx Power (mW)`	Shows the amount of light received in the transceiver.
`Rx LOS`	Shows when the received optical level falls below a preset threshold.

Related Commands

show system environment
show system pluggable
show system pluggable detail

show system serialnumber

This command shows the serial number information for the switch.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show system serialnumber`

Mode User Exec and Privileged Exec

Example To display the serial number information for the switch, use the command:

```
awplus# show system serialnumber
```

Output **Figure 8-28: Example output from the show system serialnumber command**

```
awplus#show system serialnumber
45AX5300X
```

show tech-support

This command generates system and debugging information for the switch and saves it to a file. You can optionally limit the command output to display only information for a given protocol or feature.

The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the switch we recommend saving files to either an SD card, USB storage device, or TFTP server whenever possible to avoid switch lockup. This method is not likely to be appropriate when running the working set option of ATMF across a range of physically separated switches.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

The output of this command may include the result of the following commands:

Syntax

```
show tech-support {all|[atmf|dhcpsn|epsr|igmp|ip|ipv6|mld|pim|rip|
   stack|stp|system|tacacs+]|[outfile <filename>]}
```

Parameter	Description
`all`	Display full information
`atmf`	Display ATMF- specific information
`dhcpsn`	Display DHCP Snooping specific information
`epsr`	Display EPSR specific information
`igmp`	Display IGMP specific information
`ip`	Display IP specific information
`ipv6`	Display IPv6 specific information
`mld`	Display MLD specific information
`outfile`	Output file name
`pim`	Display PIM related information
`rip`	Display Routing Information Protocol (RIP) related information
`stack`	Display stacking device information
`stp`	Display STP specific information
`system`	Display general system information
`tacacs+`	Display TACACS+ information
`|`	Output modifier
`>`	Output redirection
`>>`	Output redirection (append)
<filename>	Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.

Default Captures **all** information for the switch.

By default the output is saved to the file '`tech-support.txt.gz`' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example '`tech-support20080109.txt.gz`', so the last saved file is retained.

Usage This command is useful for collecting a large amount of information about all protocols or specific protocols on your switch so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

Mode Privileged Exec

Examples show tech-support

```
awplus# show tech-support
```

Note You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

Output The output of this command may include the result of the following commands:

show arp
show arp security
show arp security interface
show arp security statistics
show boot
show counter dhcp-client
show counter log
show counter mail
show counter ntp
show counter ping-poll
show counter snmp-server
show counter stack
show cpu
show cpu history
show diagnostic channel-group
show etherchannel
show etherchannel detail
show exception log
show interface
show interface brief
show ip dhcp snooping
show ip dhcp snooping acl
show ip dhcp snooping binding
show ip dhcp snooping interface
show ip dhcp snooping statistics
show ip igmp groups
show ip igmp interface
show ip interface
show ip route
show ip source binding
show lacp-counter

show lacp sys-id
show log
show log permanent
show memory
show memory allocations
show memory history
show memory pools
show ntp associations
show ntp status
show platform
show platform port
show power-inline
show reboot history
show running-config
show spanning-tree
show stack
show stack detail (see the **show stack** command)
show startup-config
show static-channel-group
show system
show system environment
show system pluggable
show users
show vlan brief (see the **show vlan** command)

speed (asyn)

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

Syntax `speed <console-speed-in-bps>`

Parameter	Description
<console-speed-in-bps>	Console speed Baud rate
1200	1200 Baud
2400	2400 Baud
9600	9600 Baud
19200	19200 Baud
38400	38400 Baud
57600	57600 Baud
115200	115200 Baud

Default The default console speed baud rate is 9600 bps.

Mode Line Configuration

Usage This command is used to change the console (asyn) port speed. Set the console speed to match the transmission rate of the device connected to the console (asyn) port on your switch.

Example To set the terminal console (asyn0) port speed from the switch to 57600 bps, then exit the session, and log in again to enable the change, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# speed 57600
awplus(config-line)# exit
awplus(config)# exit
awplus# exit
```

The new console speed of 57600 bps is applied after exiting the session and before login.

```
awplus login:
Password:

awplus>
```

Related Commands **line**
clear line console
show running-config

show startup-config
speed

system territory (deprecated)

This command has been deprecated in version 5.4.4-0.1. It now has no effect.

terminal monitor

Use this command to display debugging output on a terminal.

To display the cursor after a line of debugging output, press the Enter key.

Use the command **terminal no monitor** to stop displaying debugging output on the terminal, or use the timeout option to stop displaying debugging output on the terminal after a set time.

Syntax

```
terminal monitor [<1-60>]
terminal no monitor
```

Parameter	Description
<1-60>	Set a timeout between 1 and 60 seconds for terminal output.

Default Disabled

Mode User Exec and Privileged Exec

Examples To display debugging output on a terminal, enter the command:

```
awplus# terminal monitor
```

To specify timeout of debugging output after 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

To stop displaying debugging output on the terminal, use the command:

```
awplus# terminal no monitor
```

Related Commands All debug commands

undebug all

This command applies the functionality of the **no debug all** command.

Chapter 9: Debugging and Logging

Introduction 9.2
Debugging 9.2
Logging to a Terminal 9.2
Turning Off Debugging 9.3
Logging 9.3
Log Outputs 9.4

Introduction

AlliedWare Plus™ has a comprehensive debugging and logging facility in various protocols and components. This chapter describes how to start/stop debugging and logging. For detailed descriptions of the commands used to configure logging, see **Chapter 10, Logging Commands**.

Debugging

Many protocols have debug commands. Debug commands, when used with the parameters, log protocol-specific information. For example, using the **debug mstp protocol** command, results in the device writing all debugging messages generated by the MSTP algorithm to the logging system.

On using a debug command, the protocol continues to generate output until the **no** parameter is used with the command. To specify where logging output is sent, and the level of events to log, use the **log** commands in **Chapter 10, Logging Commands**.

Logging to a Terminal

To start debugging to the terminal:

Step 1: Turn on the debug options by using the relevant debug command

Step 2: Run the terminal monitor command

```
awplus> enable
awplus# configure terminal
awplus(config)# debug <protocol> (parameter)
awplus(config)# exit
awplus# terminal monitor
```

Sample Output This is a sample output of the **debug rsvp events** command displayed on the terminal:

```
awplus#terminal monitor
Dec  2 16:41:49 localhost RSVP[6518]: RSVP: RSVP message sent to
10.10.23.60/32 via interface vlan2
Dec  2 16:41:57 localhost RSVP[6518]: RSVP: Received an RSVP message
of type RSVP Reservation from 192.168.0.60 via interface vlan2
Dec  2 16:41:57 localhost RSVP[6518]: RSVP: Received a RESV message
from 10.10.23.60/32
```

Turning Off Debugging

To turn off debugging, use the `no debug` or `undebug` command. When a protocol is specified with the `no debug` or `undebug` commands, debugging is stopped for the specified protocol. To stop all debugging, use the `all` parameter with these commands.

```
awplus(config)# no debug rstp
```

or

```
awplus#undebug all
```

Logging

Protocols generate important debugging messages by default, and send them to the logging system. Additional more detailed messages can be generated by enabling debugging (**"Debugging" on page 9.2**).

Messages can be filtered based on: the program that generated the message, the severity level of the message, the type of facility that generated the message, substrings within the message text.

The severity levels in order are:

- emergencies
- alerts
- critical
- errors
- warnings
- notifications
- informational
- debugging

The facility categories are:

- auth Security/authorization messages
- authpriv Security/authorization messages (private)
- cron Clock daemon
- daemon System daemons
- ftp FTP daemon
- kern Kernel messages
- lpr Line printer subsystem
- mail Mail system
- news Network news subsystem
- syslog Messages generated internally by syslogd
- user Random user-level messages
- uucp UUCP subsystem

Log Outputs

The following types of logging output are available:

- buffered
- permanent
- terminal
- console
- host
- email

Buffered log

The buffered log is a file stored in RAM on the device. Because it is stored in RAM its content does not survive a reboot of the device. A device can only have one instance of the buffered log. The buffered log is enabled by default and has a filter to include messages with a severity level of 'notifications' and above. The buffered log can be enabled or disabled using the commands:

```
awplus# configure terminal
awplus(config)# log buffered
awplus(config)# no log buffered
```

Additional filters can be added and removed using the commands described in **log buffered (filter)** command on page 10.8:

```
awplus(config)# log buffered {facility|level|msgtext|program}
awplus(config)# no log buffered {facility|level|msgtext|
program}
```

The following log buffered commands are available:

`show log`	Displays the entire contents of the buffered log.
`show log tail`	Displays the 10 most recent entries in the buffered log.
`show log tail <10-250>`	Displays a specified number of the most recent entries in the buffered log.
`show log config`	Displays the configuration of all log outputs.
`log buffered size`	Specify the amount of memory the buffered log may use.
`clear log`	Remove the contents of the buffered log (and permanent log if it exists).
`clear log buffered`	Remove the contents of the buffered log only.
`default log buffered`	Restore the buffered log to its default configuration.

Permanent log

A device can only have one instance of the permanent log. The permanent log is enabled by default and has a filter to include messages with a severity level of 'warning' and above.

The permanent log can be disabled using the command:

```
awplus# configure terminal
awplus(config)# no log permanent
```

Additional filters can be added and removed using the commands described in **log permanent (filter)**:

```
awplus# configure terminal
awplus(config)# log permanent {facility|level|msgtext|
program}
awplus(config)# no log permanent {facility|level|msgtext|
program}
```

Table 9-1: Permanent log commands

Command	Description
`show log permanent`	Display the entire contents of the permanent log.
`show log permanent tail`	Display the 10 most recent entries in the permanent log.
`show log permanent tail <10-250>`	Display a specified number of the most recent entries in the permanent log.
`show log config`	Display the configuration of all log outputs.
`log permanent size`	Specify the amount of memory the permanent log may use.
`clear log`	Remove the contents of the buffered log and permanent log.
`clear log permanent`	Remove the contents of the permanent log only.
`default log permanent`	Restore the permanent log to its default configuration.

Host log

A host log sends log messages to a remote syslog server. A device may have many syslog hosts configured. To configure or remove a host use the commands:

```
awplus# configure terminal
awplus(config)# log host <ip-addr>9
awplus(config)# no log host <ip-addr>9
```

where `<ip-addr>` is the IP address of the remote syslog server.

There are no default filters associated with host outputs when they are created. Filters can be added and removed with the **log host (filter)** command on page 10.23.

It is not possible to view the log messages sent to this type of output as they are not retained on the device. They must be viewed on the remote device. The other host log commands are:

`show log config`	Displays the configuration of all log outputs.
`log host time`	Adjust the time information in messages to a time zone other than the one configured on this device.
`default log host <ip-address>`	Restores the device default settings for log sent to a remote syslog server.

Email log

An email log sends log messages to an email address. A device may have many email logs configured. To configure or remove an email log use the commands:

```
awplus# configure terminal
awplus(config)# log email <email-address>
awplus(config)# no log email <email-address>
```

where `<email-address>` is the destination email address.

There are no default filters associated with email outputs when they are created. Filters can be added and removed with the commands described in **log email (filter)**:

```
awplus# configure terminal
awplus(config)# log email <email-address> {facility|level|
msgtext|program}
awplus(config)# no log email <email-address> {facility|
level|msgtext|program}
```

It is not possible to view the log messages sent to this type of output as they are not retained on the device. They must be viewed by the email recipient.

The other email log commands are:

`show log config`	Displays the configuration of all log outputs.
`log email time`	Adjust the time information in messages to a time zone other than the one configured on this device.
`default log email`	Restores the device default settings for log messages sent to an email address.

Note

An email server and "from" address must be configured on the device in order for email logs to work:

- mail from <*email-address*>
- mail smtpserver <*ip-address*>

where the <*email-address*> is the 'From:' field on the sent email, and the <*ip-address*> is the email's destination SMTP server.

Email logs are sent in batches of approximately 20 messages and have the subject line "Log messages"

Chapter 10: Logging Commands

Command List 10.2
clear exception log 10.2
clear log 10.2
clear log buffered 10.3
clear log permanent 10.3
default log buffered 10.4
default log console 10.4
default log email 10.5
default log host 10.5
default log monitor 10.6
default log permanent 10.6
log buffered 10.7
log buffered (filter) 10.8
log buffered size 10.11
log console 10.12
log console (filter) 10.13
log email 10.16
log email (filter) 10.17
log email time 10.20
log host 10.22
log host (filter) 10.23
log host time 10.26
log monitor (filter) 10.28
log permanent 10.30
log permanent (filter) 10.31
log permanent size 10.33
log-rate-limit nsm 10.34
show counter log 10.35
show exception log 10.36
show log 10.37
show log config 10.39
show log permanent 10.42
show running-config log 10.43

Command List

This chapter provides an alphabetical reference of commands used to configure logging.

clear exception log

This command resets the contents of the exception log, but does not remove the associated core files.

Note When this command is used within a stacked environment, it will remove the contents of the exception logs in all stack members.

Syntax `clear exception log`

Mode Privileged Exec

Example

```
awplus# clear exception log
```

clear log

This command removes the contents of the buffered and permanent logs.

Note When this command is used within a stacked environment, it will remove the contents of the buffered and permanent logs in all stack members.

Syntax `clear log`

Mode Privileged Exec

Example To delete the contents of the buffered and permanent log use the command:

```
awplus# clear log
```

Validation Commands **show log**

Related Commands **clear log buffered**
clear log permanent

clear log buffered

This command removes the contents of the buffered log.

Note When this command is used within a stacked environment, it will remove the contents of the buffered logs in all stack members.

Syntax `clear log buffered`

Mode Privileged Exec

Example To delete the contents of the buffered log use the following commands:

```
awplus# clear log buffered
```

Validation Commands **show log**

Related Commands **clear log**
clear log permanent

clear log permanent

This command removes the contents of the permanent log.

Note When this command is used within a stacked environment, it will remove the contents of the buffered logs in all stack members.

Syntax `clear log permanent`

Mode Privileged Exec

Example To delete the contents of the permanent log use the following commands:

```
awplus# clear log permanent
```

Validation Commands **show log**

Related Commands **clear log**
clear log buffered

default log buffered

This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of "warnings" and above.

Syntax `default log buffered`

Default The buffered log is enabled by default.

Mode Global Configuration

Example To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

Validation Commands **show log config**

Related Commands **log buffered**
log buffered size

default log console

This command restores the default settings for log messages sent to the terminal when a **log console** command is issued. By default all messages are sent to the console when a **log console** command is issued.

Syntax `default log console`

Mode Global Configuration

Example To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

Validation Commands **show log config**

Related Commands **log console**
log console (filter)

default log email

This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax `default log email <email-address>`

Parameter	Description
<email-address>	The email address to send log messages to

Mode Global Configuration

Example To restore the default settings for log messages sent to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related Commands **show log config**

default log host

This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax `default log host <ip-addr>`

Parameter	Description
<ip-addr>	The IP address of a remote syslog server

Mode Global Configuration

Example To restore the default settings for messages sent to the remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

Validation Commands **show log config**

Related Commands **log email**

default log monitor

This command restores the default settings for log messages sent to the terminal when a **terminal monitor** command is used.

Syntax `default log monitor`

Default All messages are sent to the terminal when a **terminal monitor** command is used.

Mode Global Configuration

Example To restore the log monitor to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log monitor
```

Related Commands
log monitor (filter)
show log config

default log permanent

This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of `warnings` and above.

Syntax `default log permanent`

Default The permanent log is enabled by default.

Mode Global Configuration

Example To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

Related Commands
log permanent
log permanent size
show log config

log buffered

This command configures the device to store log messages in RAM. Messages stored in RAM are not retained on the device over a restart. Once the buffered log reaches its configured maximum allowable size old messages will be deleted to make way for new ones.

Syntax

```
log buffered
no log buffered
```

Default The buffered log is configured by default.

Mode Global Configuration

Examples To configured the device to store log messages in RAM use the following commands:

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

To configure the device to not store log messages in a RAM buffer use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered
```

Validation Commands **show log config**

Related Commands **default log buffered**
log buffered (filter)
log buffered size

log buffered (filter)

Use this command to create a filter to select messages to be sent to the buffered log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the buffered log.

Syntax

```
log buffered [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]

no log buffered [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
`level`	Filter messages to the buffered log by severity level.
<level>	The minimum severity of message to send to the buffered log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0 emergencies: System is unusable 1 alerts Action must be taken immediately 2 critical Critical conditions 3 errors Error conditions 4 warnings Warning conditions 5 notices Normal, but significant, conditions 6 informational Informational messages 7 debugging Debug-level messages
`program`	Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output. rip Routing Information Protocol (RIP) rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control lacp Link Aggregation Control Protocol (LACP) stp Spanning Tree Protocol (STP) rstp Rapid Spanning Tree Protocol (RSTP) mstp Multiple Spanning Tree Protocol (MSTP) imi Integrated Management Interface (IMI) imish Integrated Management Interface Shell (IMISH) epsr Ethernet Protection Switched Rings (EPSR) rmon Remote Monitoring loopprot Loop Protection poe Power-inline (Power over Ethernet) dhcpsn DHCP snooping (DHCPSN)

Parameter	Description
`facility`	Filter messages to the buffered log by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from in the buffered log: kern — Kernel messages user — Random user-level messages mail — Mail system daemon — System daemons auth — Security/authorization messages syslog — Messages generated internally by syslogd lpr — Line printer subsystem news — Network news subsystem uucp — UUCP subsystem cron — Clock daemon authpriv — Security/authorization messages (private) ftp — FTP daemon
`msgtext`	Select messages containing a certain text string (maximum 128 characters).
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the buffered log has a filter to select messages whose severity level is "notices (5)" or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages generated by EPSR that have a severity of `notices` or higher to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered level notices program epsr
```

To add a filter to send all messages containing the text "`Bridging initialization`", to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered msgtext Bridging initialization
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered level notices program epsr
```

To remove a filter that sends all messages containing the text "`Bridging initialization`", to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

Validation Commands **show log config**

Related Commands **default log buffered**
log buffered
log buffered size

log buffered size

This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Syntax `log buffered size <50-250>`

Parameter	Description
<50-250>	Size of the RAM log in kilobytes

Mode Global Configuration

Example To allow the buffered log to use up to 100 kB of RAM use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered size 100
```

Validation Commands **show log config**

Related Commands **default log buffered**
log buffered

log console

This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the devices main console port.

Use the **no** variant of this command to configure the device not to send log messages to consoles.

Syntax

```
log console
no log console
```

Mode Global Configuration

Examples To configure the device to send log messages use the following commands:

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

To configure the device not to send log messages in all consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console
```

Validation Commands show log config

Related Commands log console (filter)

log console (filter)

This command creates a filter to select messages to be sent to all consoles when the log console command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log console [level <level>] [program <program-name>]
    [facility <facility>] [msgtext <text-string>]

no log console [level <level>] [program <program-name>]
    [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
`level`	Filter messages by severity level.
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0 emergencies: System is unusable 1|alerts Action must be taken immediately 2|critical Critical conditions 3|errors Error conditions 4|warnings Warning conditions 5|notices Normal, but significant, conditions 6|informational Informational messages 7|debugging Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output. rip Routing Information Protocol (RIP) rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control lacp Link Aggregation Control Protocol (LACP) stp Spanning Tree Protocol (STP) rstp Rapid Spanning Tree Protocol (RSTP) mstp Multiple Spanning Tree Protocol (MSTP) imi Integrated Management Interface (IMI) imish Integrated Management Interface Shell (IMISH) epsr Ethernet Protection Switched Rings (EPSR) rmon Remote Monitoring loopprot Loop Protection poe Power-inline (Power over Ethernet) dhcpsn DHCP snooping (DHCPSN)
`facility`	Filter messages to the buffered log by syslog facility.

Parameter	Description	
<facility>	Specify one of the following syslog facilities to include messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
`msgtext`	Select messages containing a certain text string	
<text-string>	A text string to match. This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is `critical` or higher. This filter may be removed using the **no** variant of this command. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages generated by MSTP that have a severity of `info` or higher to console instances where the log console command has been given, remove the default filter that includes everything use the following commands:

```
awplus# configure terminal
awplus(config)# log console level info program mstp
```

and then use the command:

```
awplus(config)# log console level info program mstp
```

To create a filter to send all messages containing the text "`Bridging initialization`" to console instances where the log console command has been given use the following commands:

```
awplus# configure terminal
awplus(config)# log console msgtext "Bridging initialization"
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level notices program epsr
```

To remove a default filter that includes sending `critical`, `alert` and `emergency` level messages to the console use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

Validation Commands **show log config**

Related Commands **log console**

log email

This command configures the device to send log messages to an email address. The email address is specified in this command.

Syntax `log email <email-address>`

Parameter	Description
<email-address>	The email address to send log messages to

Default By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

Mode Global Configuration

Example To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

Validation Commands **show log config**

Related Commands **default log email**
log email

log email (filter)

This command creates a filter to select messages to be sent to an email address. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a specified email address. All configuration relating to this log target will be removed.

Syntax

```
log email <email-address> [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]

no log email <email-address> [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
<email-address>	The email address to send logging messages to
`level`	Filter messages by severity level.
<level>	The minimum severity of messages to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0 emergencies: System is unusable 1 alerts Action must be taken immediately 2 critical Critical conditions 3 errors Error conditions 4 warnings Warning conditions 5 notices Normal, but significant, conditions 6 informational Informational messages 7 debugging Debug-level messages
`program`	Filter messages by program. Include messages from a specified program in the log.

Parameter	Description
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case -sensitive) that you find in the log output. rip Routing Information Protocol (RIP) rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control lacp Link Aggregation Control Protocol (LACP) stp Spanning Tree Protocol (STP) rstp Rapid Spanning Tree Protocol (RSTP) mstp Multiple Spanning Tree Protocol (MSTP) imi Integrated Management Interface (IMI) imish Integrated Management Interface Shell (IMISH) epsr Ethernet Protection Switched Rings (EPSR) rmon Remote Monitoring loopprot Loop Protection poe Power-inline (Power over Ethernet) dhcpsn DHCP snooping (DHCPSN)
`facility`	Filter messages to the log by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from in the log: kern Kernel messages user Random user-level messages mail Mail system daemon System daemons auth Security/authorization messages syslog Messages generated internally by syslogd lpr Line printer subsystem news Network news subsystem uucp UUCP subsystem cron Clock daemon authpriv Security/authorization messages (private) ftp FTP daemon
`msgtext`	Select messages containing a certain text string
<text-string>	A text string to match. This is case sensitive, and must be the last text on the command line.

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com level notices
program epsr
```

To create a filter to send all messages containing the text "`Bridging initialization`", to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext
"Bridging initialization"
```

To create a filter to send messages with a severity level of `informational` and above to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level
informational
```

To stop the device emailing log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com level
notices program epsr
```

To remove a filter that sends messages with a severity level of `informational` and above to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level
informational
```

Related Commands **default log email**
log email
show log config

log email time

This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your switch then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

```
log email <email-address> time {local|local-offset|utc-offset {plus|
   minus}<0-24>}
```

Parameter	Description
<email-address>	The email address to send log messages to
`time`	Specify the time difference between the email recipient and the switch you are configuring.
`local`	The switch is in the same time zone as the email recipient
`local-offset`	The switch is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from local time of the switch to the email recipient in hours.
`utc-offset`	The switch is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from UTC time of the switch to the email recipient in hours.
`plus`	Negative offset (difference) from the switch to the email recipient.
`minus`	Positive offset (difference) from the switch to the email recipient.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

Examples To send messages to the email address `test@home.com` in the same time zone as the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset
plus 3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the switch's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset
minus 3
```

Validation Commands **show log config**

Related Commands **default log buffered**

log host

This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

Syntax

```
log host <ip-addr>
no log host <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of a remote syslog server in dotted decimal format A.B.C.D

Mode Global Configuration

Examples To configure the device to send log messages to a remote syslog server with IP address `10.32.16.99` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.99
```

To stop the device from sending log messages to the remote syslog server with IP address `10.32.16.99` use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.99
```

Validation Commands **show log config**

Related Commands **default log host**

log host (filter)

This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

Syntax

```
log host <ip-addr> [level <level>] [program <program-name>]
    [facility <facility>] [msgtext <text-string>]

no log host <ip-addr> [level <level>] [program <program-name>]
    [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
<ip-addr>	The IP address of a remote syslog server
`level`	Filter messages by severity level.
<level>	The minimum severity of messages to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0|emergencies: System is unusable 1|alerts Action must be taken immediately 2|critical Critical conditions 3|errors Error conditions 4|warnings Warning conditions 5|notices Normal, but significant, conditions 6|informational Informational messages 7|debugging Debug-level messages
`program`	Filter messages by program. Include messages from a specified program in the log.
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case -sensitive) that you find in the log output. rip Routing Information Protocol rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control

Parameter	Description	
`<program-name>` (cont.)	lacp	Link Aggregation Control Protocol (LACP)
	stp	Spanning Tree Protocol (STP)
	rstp	Rapid Spanning Tree Protocol (RSTP)
	mstp	Multiple Spanning Tree Protocol (MSTP)
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
`facility`	Filter messages to the log by syslog facility.	
`<facility>`	Specify one of the following syslog facilities to include messages from in the log:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
`msgtext`	Select messages containing a certain text string	
`<text-string>`	A text string to match. This is case sensitive, and must be the last text on the command line.	

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level notices program epsr
```

To create a filter to send all messages containing the text "`Bridging initialization`", to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of `informational` and above to the syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 level notices program
epsr
```

To remove a filter that sends all messages containing the text "`Bridging initialization`", to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of `informational` and above to the syslog server with IP address `10.32.16.21` use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Related Commands

default log host
show log config

log host time

This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your switch then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

```
log host <email-address> time {local|local-offset|utc-offset {plus|
   minus} <0-24>}
```

Parameter	Description
<email-address>	The email address to send log messages to
`time`	Specify the time difference between the email recipient and the switch you are configuring.
`local`	The switch is in the same time zone as the email recipient
`local-offset`	The switch is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from local time of the switch to the email recipient in hours.
`utc-offset`	The switch is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from UTC time of the switch to the email recipient in hours.
`plus`	Negative offset (difference) from the switch to the syslog server.
`minus`	Positive offset (difference) from the switch to the syslog server.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage Use the **local** option if the remote syslog server is in the same time zone as the switch. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

Examples To send messages to the remote syslog server with the IP address `10.32.16.21` in the same time zone as the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address `10.32.16.12` with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the switch's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address `10.32.16.02` with the time information converted to the time zone of the email recipient, which is 3 hours behind the switch's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Validation Commands **show log config**

Related Commands **default log buffered**

log monitor (filter)

This command creates a filter to select messages to be sent to the terminal when the terminal monitor command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log monitor [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]

no log monitor [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
`level`	Filter messages to the permanent log by severity level.
<level>	The minimum severity of message to send to the log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0|emergencies: System is unusable 1|alerts Action must be taken immediately 2|critical Critical conditions 3|errors Error conditions 4|warnings Warning conditions 5|notices Normal, but significant, conditions 6|informational Informational messages 7|debugging Debug-level messages
`program`	Filter messages to the permanent log by program. Include messages from a specified program in the log.
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case -sensitive) that you find in the log output. rip Routing Information Protocol (RIP) rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control lacp Link Aggregation Control Protocol (LACP) stp Spanning Tree Protocol (STP) rstp Rapid Spanning Tree Protocol (RSTP) mstp Multiple Spanning Tree Protocol (MSTP) imi Integrated Management Interface (IMI)
<program-name> `(cont.)`	imish Integrated Management Interface Shell (IMISH) epsr Ethernet Protection Switched Rings (EPSR) rmon Remote Monitoring loopprot Loop Protection poe Power-inline (Power over Ethernet) dhcpsn DHCP snooping (DHCPSN)
`facility`	Filter messages to the permanent log by syslog facility.

Parameter	Description	
<facility>	Specify one of the following syslog facilities to include messages from in the log:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
`msgtext`	Select messages containing a certain text string	
<text-string>	A text string to match. This is case sensitive, and must be the last text on the command line.	

Default By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages generated by MSTP that have a severity of `info` or higher to terminal instances where the terminal monitor command has been given use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor level info program mstp
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to the terminal use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level notices program epsr
```

To remove a default filter that includes sending everything to the terminal use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

Validation Commands **show log config**

Related Commands **terminal monitor**

log permanent

This command configures the device to send permanent log messages to non-volatile storage (NVS) on the device. The content of the permanent log is retained over a reboot. Once the permanent log reaches its configured maximum allowable size old messages will be deleted to make way for new messages.

The **no** variant of this command configures the device not to send any messages to the permanent log. Log messages will not be retained over a restart.

Syntax

```
log permanent
no log permanent
```

Mode Global Configuration

Examples To enable permanent logging use the following commands:

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

To disable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# no log permanent
```

Validation Commands **show log config**

Related Commands **default log permanent**
log permanent (filter)
log permanent size
show log permanent

log permanent (filter)

This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the permanent log.

Syntax

```
log permanent [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]

no log permanent [level <level>] [program <program-name>]
   [facility <facility>] [msgtext <text-string>]
```

Parameter	Description
`level`	Filter messages to the permanent log by severity level.
<level>	The minimum severity of message to send to the log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: 0|emergencies: System is unusable 1|alerts Action must be taken immediately 2|critical Critical conditions 3|errors Error conditions 4|warnings Warning conditions 5|notices Normal, but significant, conditions 6|informational Informational messages 7|debugging Debug-level messages
`program`	Filter messages to the permanent log by program. Include messages from a specified program in the log.
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case -sensitive) that you find in the log output. rip Routing Information Protocol (RSVP) rsvp Resource Reservation Protocol (RSVP) dot1x IEEE 802.1X Port-Based Access Control lacp Link Aggregation Control Protocol (LACP) stp Spanning Tree Protocol (STP) rstp Rapid Spanning Tree Protocol (RSTP) mstp Multiple Spanning Tree Protocol (MSTP) imi Integrated Management Interface (IMI) imish Integrated Management Interface Shell (IMISH) epsr Ethernet Protection Switched Rings (EPSR) rmon Remote Monitoring loopprot Loop Protection poe Power-inline (Power over Ethernet) dhcpsn DHCP snooping (DHCPSN)

Parameter	Description	
`facility`	Filter messages to the permanent log by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from in the log:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
`msgtext`	Select messages containing a certain text string	
<text-string>	A text string to match. This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is `notices (5)` or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to the permanent log use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent level notices program epsr
```

To create a filter to send all messages containing the text "`Bridging initialization`", to the permanent log use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent msgtext Bridging initialization
```

Validation Commands **show log config**

Related Commands **default log permanent**
log permanent
log permanent size
show log permanent

log permanent size

This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Syntax `log permanent size <50-250>`

Parameter	Description
<50-250>	Size of the permanent log in kilobytes

Mode Global Configuration

Example To allow the permanent log to use up to 100 kB of NVS use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent size 100
```

Validation Commands **show log config**

Related Commands **default log permanent**
log permanent

log-rate-limit nsm

This command limits the number of log messages generated by the switch for a given interval.

Use the **no** variant of this command to revert to the default number of log messages generated by the switch of up to 200 log messages per second.

Syntax

```
log-rate-limit nsm messages <message-limit> interval <time-interval>
no log-rate-limit nsm
```

Parameter	Description
<message-limit>	<1-65535> The number of log messages generated by the switch.
<time-interval>	<0-65535> The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied.

Default By default, the switch will allow 200 log messages to be generated per second.

Mode Global Configuration

Usage Previously, if the switch received a continuous stream of IGMP packets with errors, such as when a packet storm occurs because of a network loop, then the switch generates a lot of log messages using more and more memory, which may ultimately cause the switch to shutdown. This log rate limiting feature constrains the rate that log messages are generated by the switch.

Note that if within the given time interval, the number of log messages exceeds the limit, then any excess log messages are discarded. At the end of the time interval, a single log message is generated indicating that log messages were discarded due to the log rate limit being exceeded.

Thus if the expectation is that there will be a lot of discarded log messages due to log rate limiting, then it is advisable to set the time interval to no less than 100, which means that there would only be one log message, indicating log excessive log messages have been discarded.

Examples To limit the switch to generate up to 300 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# log-rate-limit nsm messages 300 interval 100
```

To return the switch the default setting, to generate up to 200 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# no log-rate-limit nsm
```

show counter log

This command displays log counter information.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show counter log`

Mode User Exec and Privileged Exec

Example To display the log counter information, use the command:

```
awplus# show counter log
```

Output **Figure 10-1: Example output from the show counter log command**

```
Log counters
Total Received          ......... 2328
Total Received P0       ......... 0
Total Received P1       ......... 0
Total Received P2       ......... 1
Total Received P3       ......... 9
Total Received P4       ......... 32
Total Received P5       ......... 312
Total Received P6       ......... 1602
Total Received P7       ......... 372
```

Table 10-1: Parameters in output of the show counter log command

Parameter	Description
`Total Received`	Total number of messages received by the log
`Total Received P0`	Total number of Priority 0 (Emergency) messages received
`Total Received P1`	Total number of Priority 1 (Alert) messages received
`Total Received P2`	Total number of Priority 2 (Critical) messages received
`Total Received P3`	Total number of Priority 3 (Error) messages received
`Total Received P4`	Total number of Priority 4 (Warning) messages received
`Total Received P5`	Total number of Priority 5 (Notice) messages received
`Total Received P6`	Total number of Priority 6 (Info) messages received
`Total Received P7`	Total number of Priority 7 (Debug) messages received

Related Commands **show log config**

show exception log

This command displays the contents of the exception log. When used within a stacked environment, this command will display the contents of the exception log for all the stack members.

Syntax `show exception log`

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output **Figure 10-2: Example output from the show exception log command on a switch**

```
awplus#show exception log

Stack member 1:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Jan 27 09:57:47 local7.debug awplus corehandler : Process imish (PID:3746)
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-3746.tgz
2014 Jan 27 09:57:47 local7.debug awplus corehandler : Process imish (PID:2504)
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-2504.tgz
2014 Jan 27 09:58:02 local7.debug awplus corehandler : Process ospfd (PID:1512)
signal 5, core dumped to /flash/ospfd-x610-5.4.3-3.7-1-1390816682-1512.tgz
------------------------------------------------------------------------
Stack member 2:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Jan 27 09:58:16 local7.debug awplus-2 corehandler : Process imi (PID:1427)
signal 5, core dumped to /flash/imi-x610-5.4.3-3.7-2-1390816696-1427.tgz
------------------------------------------------------------------------
```

show log

This command displays the contents of the buffered log.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show log [tail [<10-250>]]`

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default By default the entire contents of the buffered log is displayed.

Mode User Exec, Privileged Exec and Global Configuration

Usage If the optional **tail** parameter is specified only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.

Examples To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

Output **Figure 10-3: Example output from the show log command**

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------
2011 Aug 29 07:55:22 kern.notice awplus kernel: Linux version 2.6.32.12-at1 (mak
er@awpmaker03-dl) (gcc version 4.3.3 (Gentoo 4.3.3-r3 p1.2, pie-10.1.5) ) #1 Wed
 Dec 8 11:53:40 NZDT 2010
2011 Aug 29 07:55:22 kern.warning awplus kernel: No pci config register base in
dev tree, using default
2011 Aug 29 07:55:23 kern.notice awplus kernel: Kernel command line: console=tty
S0,9600 releasefile=GS900-5.4.4E-1.1.rel ramdisk=14688 bootversion=1.1.0-rc12
loglevel=1
 extraflash=00000000
2011 Aug 29 07:55:25 kern.notice awplus kernel: RAMDISK: squashfs filesystem fou
nd at block 0
2011 Aug 29 07:55:28 kern.warning awplus kernel: ipifwd: module license 'Proprie
tary' taints kernel.
.
.
.
```

Figure 10-4: Example output from the show log tail command

```
awplus#show log tail

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------
2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 469 cmd logrotate /
etc/logrotate.conf
2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 471 cmd nbqueue --
wipe
2006 Nov 10 13:35:01 cron.notice crond[116]: USER manager pid 472 cmd nbqueue --
wipe
2006 Nov 10 13:40:01 cron.notice crond[116]: USER manager pid 477 cmd nbqueue --
wipe
2006 Nov 10 13:44:36 syslog.notice syslog-ng[67]: Log statistics;
processed=\'center(queued)=70\', processed=\'2006 Nov 10 13:45:01 cron.notice
crond[116]: USER manager pid 478 cmd logrotate /etc/logrotate.conf
2006 Nov 10 13:45:01 cron.notice crond[116]: USER manager pid 480 cmd nbqueue --
wipe
2006 Nov 10 13:49:32 syslog.notice syslog-ng[67]: SIGHUP received, reloading
configuration;
2006 Nov 10 13:50:01 cron.notice crond[116]: USER manager pid 482 cmd nbqueue --
wipe
2006 Nov 10 13:55:01 cron.notice crond[116]: USER manager pid 483 cmd nbqueue --
wipe
.
.
.
```

Related Commands **show log config**
show log permanent

show log config

This command displays information about the logging system. This includes the configuration of the various log destinations, buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each of these destinations.

Syntax `show log config`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the logging configuration use the command:

```
awplus# show log config
```

Output **Figure 10-5: Example output from the show log config command**

```
Buffered log:
Status ......... enabled
  Maximum size ... 100kb
  Filters:
 *1 Level ........ notices
    Program ...... any
    Facility ..... any
    Message text . any
  2 Level ........ informational
    Program ...... mstp
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2006 Dec 11
10:36:16)
Permanent log:
  Status ......... enabled
  Maximum size ... 60kb
  Filters:
  1 Level ........ error
    Program ...... any
    Facility ..... any
    Message text . any
 *2 Level ........ warnings
    Program ...... dhcp
    Facility ..... any
    Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2006 Dec 11
10:36:16)
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Filters:
  1 Level ........ critical
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2006 Dec 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ........ emergencies
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2006 Dec 11
10:36:16)
Monitor log:
  Filters:
 *1   Level ...... debugging
      Program .... any
      Facility ... any
      Msg text ... any
  Statistics ..... Not available
Console log:
  Status ......... enabled
  List of consoles:
  1 .............. ttyS0
  Filters:
 *1   Level ...... critical
      Program .... any
      Facility ... any
      Msg text ... any
  Statistics ..... 1327 messages received, 1 accepted by filter (2006 Dec 11
10:36:16)
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with "*'.

Note

Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.

Related Commands

show counter log
show log
show log permanent

show log permanent

This command displays the contents of the permanent log.

When used within a stacked environment, this command will display the contents of the permanent log for all the stack members, unless you specify a particular stack member.

Syntax `show log permanent[<stack-ID>][tail [<10-250>]]`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default If the optional `tail` parameter is specified only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the `tail` parameter to select how many of the latest messages should be displayed.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the permanent log of stack member 2, use the command:

```
awplus# show log permanent 2
```

Output **Figure 10-6: Example output from the show log permanent command**

```
awplus#show log permanent 2

Stack member 2:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-------------------------------------------------------------------------

2014 Feb 25 09:10:48 daemon.crit awplus-2 HPI: HOTSWAP Pluggable 2.0.51 hotswapped
in: AT-StackXS/1.0
2014 Feb 25 09:10:48 daemon.crit awplus-2 HPI: HOTSWAP Pluggable 2.0.52 hotswapped
in: 2127931-2
2014 Feb 25 09:10:50 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has
joined the stack
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has
become the Active Master
2014 Feb 25 09:10:52 local6.alert awplus-2 VCS[922]: stack member has booted from
non-default location, SW version auto synchronization cannot be supported.
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Stack Virtual MAC is
0000.cd37.0002
2014 Feb 25 09:11:46 user.crit awplus-2 ATMF[862]: awplus-x510 has joined. 1
member in total.
```

Related Commands show log

show running-config log

This command displays the current running configuration of the Log utility.

Syntax `show running-config log`

Mode Privileged Exec and Global Configuration

Example To display the current configuration of the log utility, use the command:

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

Related Commands **show log**
show log config

Chapter 11: Scripting Commands

Command List 11.2
activate 11.2
echo 11.3
wait 11.4

Command List

This chapter provides commands used for command scripts.

activate

This command activates a script file.

Syntax `activate [background] <script>`

Parameter	Description
`background`	Activate a script to run in the background. A process that is running in the background will operate as a separate task, and will not interrupt foreground processing. Generally, we recommend running short, interactive scripts in the foreground and longer scripts in the background. The default is to run the script in the foreground.
<script>	The file name of the script to activate. The script is a command script consisting of commands documented in this software reference. Note that you must use either a **.scp** or a **.sh** filename extension for a valid script text file, as described below in the usage section for this command.

Mode Privileged Exec

Usage When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an **enable (Privileged Exec mode)** command to the start of your script. If you need to run Global Configuration commands in your script you need to add a **configure terminal** command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A **terminal length** shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **.sh** or **.scp** only for the AlliedWare Plus™ CLI to activate the script file. The **.sh** filename extension indicates the file is an ASH script, and the **.scp** filename extension indicates the file is an AlliedWare Plus™ script.

Examples To activate a command script to run as a background process, use the command:

```
awplus# activate background test.scp
```

Related Commands
configure terminal
echo
enable (Privileged Exec mode)
wait

echo

This command echoes a string to the terminal, followed by a blank line.

Syntax `echo <line>`

Parameter	Description
<line>	The string to echo

Mode User Exec and Privileged Exec

Usage This command may be useful in CLI scripts, to make the script print user-visible comments.

Example To echo the string `Hello World` to the console, use the command:

```
awplus# echo Hello World
```

Output

```
Hello World
```

Related Commands **activate**
wait

wait

This command pauses execution of the active script for the specified period of time.

Syntax `wait <delay>`

Parameter	Description
<delay>	<1-65335> Specify the time delay in seconds

Default No wait delay is specified by default to pause script execution.

Mode Privileged Exec (when executed from a script not directly from the command line)

Usage Use this command to pause script execution in an **.scp** (AlliedWare Plus™ script) or an **.sh** (ASH script) file executed by the **activate** command. The script must contain an **enable (Privileged Exec mode)** command since the **wait** command is only executed in the Privileged Exec mode.When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an **enable (Privileged Exec mode)** command to the start of your script.

Related Commands
activate
echo
enable (Privileged Exec mode)

Chapter 12: Interface Commands

Command List 12.2
description (interface) 12.2
interface (to configure) 12.3
mru 12.5
mtu 12.7
show interface 12.9
show interface brief 12.12
show interface status 12.13
shutdown 12.15

Command List

This chapter provides an alphabetical reference of commands used to configure and display interfaces.

description (interface)

Use this command to add a description to a specific port or interface.

Syntax `description <description>`

Parameter	Description
<description>	Text describing the specific interface.

Mode Interface Configuration

Example The following example uses this command to describe the device that a switch port is connected to.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# description Boardroom PC
```

interface (to configure)

Use this command to select one or more interfaces to configure.

Syntax

```
interface <interface-list>
interface lo
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface such as a VLAN (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`lo`	The local loopback interface.

Usage

A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the switch and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

One example of this increased reliability is for OSPF to advertise a local loopback interface as an interface-route into the network irrespective of the physical links that may be “up” or “down” at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded.

Mode

Global Configuration

Example

The following example shows how to enter Interface mode to configure `vlan1`. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

Related Commands

ip address
show interface
show interface brief

mru

Use this command to set the Maximum Receive Unit (MRU) size for switch ports, where MRU is the maximum frame size (excluding headers) that switch ports can receive. For more information, see **"Support for Jumbo Frames" on page 14.16**.

Use the **no** variant of this command to remove a previously specified Maximum Receive Unit (MRU) size for switch ports, and restore the default MRU size (1500 bytes) for switch ports.

Note

The figure of 1500 bytes specifies the payload only. For an IEEE 802.1q frame, provision is made (internally) for the following additional components:

- Source and Destination addresses
- EtherType field
- Priority and VLAN tag fields
- FCS

These additional components increase the frame size internally to 1522 bytes.

Syntax

```
mru <mru-size>
no mru
```

Parameter	Description
<mru-size>	<68-16357> Specifies the Maximum Receive Unit (MRU) size in bytes, where 1500 bytes is the default Ethernet MRU size for an interface.

Default The default MRU size is 1500 bytes for switch ports.

Mode Interface Configuration for switch ports.

Usage Note that **show interface** output will only show MRU size for switch ports.

Examples To configure an MRU of 16357 bytes on `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru 16357
```

To configure an MRU of 1500 bytes on `port1.0.2` to `port1.0.4` use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# mru 1500
```

To restore the MRU size of 1500 bytes on `port1.0.2`, use the commands:

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

Related Commands **show interface**

mtu

Use this command to set the Maximum Transmission Unit (MTU) size for VLANs, where MTU is the maximum packet size that VLANs can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size for VLANs, and restore the default MTU size (1500 bytes) for VLANs.

Syntax

```
mtu <mtu-size>
no mtu
```

Parameter	Description
<mtu-size>	<68-1582> Specifies the Maximum Transmission Unit (MTU) size in bytes, where 1500 bytes is the default Ethernet MTU size for an interface.

Default The default MTU size is 1500 bytes for VLAN interfaces.

Mode Interface Configuration for VLAN interfaces.

Usage If a switch receives an IPv4 packet for Layer 3 switching to another VLAN with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the switch will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting VLAN interface, an ICMP '**packet too big**' (ICMP type 2 code 0) message is sent to the source.

Note that **show interface** output will only show MTU size for VLAN interfaces.

Examples To configure an MTU size of 1500 bytes on interface `vlan2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# mtu 1500
```

To configure an MTU size of 1500 bytes on interfaces `vlan2` to `vlan4`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# mtu 1500
```

To restore the MTU size to the default MTU size of 1500 bytes on `vlan2`, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no mtu
```

To restore the MTU size to the default MTU size of 1500 bytes on `vlan2` and `vlan4`, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no mtu
```

Related Commands **show interface**

show interface

Use this command to display interface configuration and status.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface such as a VLAN (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`lo`	The local loopback interface.

Mode User Exec and Privileged Exec

Usage Note that the output displayed with this command will show MTU (Maximum Transmission Unit) size for VLAN interfaces, and MRU (Maximum Received Unit) size for switch ports.

Example To display configuration and status information for all interfaces, use the command:

```
awplus# show interface
```

Figure 12-1: Example output from the show interface command

```
awplus#show interface
Interface port1.0.1
  Scope: both
  Link is UP, administrative state is UP
  Thrash-limiting
    Status Not Detected, Action link-down, Timeout 60(s)
  Hardware is Ethernet, address is 0000.cd24.daeb
  index 5001 metric 1 mru 1500
  <UP,BROADCAST,RUNNING,MULTICAST>
  current duplex half, current speed 100
  configured duplex auto, configured speed auto, configured polarity auto
  current ecofriendly lpi
  configured ecofriendly lpi
  SNMP link-status traps: Sending (Suppressed after 20 traps in 60 sec.)
    input packets 2396, bytes 324820, dropped 0, multicast packets 2370
    output packets 73235, bytes 406566, multicast packets 7321 broadcast packets 7
  Time since last state change: 0 days 16:35:52

Interface port2.0.2
  Scope: both
  Link is DOWN, administrative state is UP
  Thrash-limiting
    Status Unknown, Action learn-disable, Timeout 1(s)
  Hardware is Provisioned, address is 0000.0000.0000
  index 8001 metric 1 mru 1500
  <BROADCAST,MULTICAST>
  current duplex half, current speed 100
  configured duplex auto, configured speed auto, configured polarity auto
  current ecofriendly lpi
  configured ecofriendly lpi
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 16:35:52


Interface lo
  Scope: both
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 16:35:52

Interface vlan1
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0000.cd24.daa8
  index 201 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 29, bytes 1334, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 05:36:40
```

To display configuration and status information for interface `lo`, use the command:

```
awplus# show interface lo
```

Figure 12-2: Example output from the show interface lo command

```
awplus#show interface lo
Interface lo
  Scope: both
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 69 days 01:28:47
```

To display configuration and status information for interfaces `vlan1` and `vlan2`, use the command:

```
awplus# show interface vlan1,vlan2
```

Figure 12-3: Example output from the show interface vlan1,vlan2 command

```
awplus#show interface vlan1,vlan2
Interface vlan1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is VLAN, address is 0015.77e9.5c50
  IPv4 address 192.168.1.1/24 broadcast 192.168.1.255
  index 201 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 295606, bytes 56993106, dropped 5, multicast packets 156
    output packets 299172, bytes 67379392, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 14:22:39

 Interface vlan2
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0015.77e9.5c50
  IPv4 address 192.168.2.1/24 broadcast 192.168.2.255
  Description: ip_phone_vlan
  index 202 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 90, bytes 4244, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 14:22:39
```

Related Commands

- **ecofriendly lpi**
- **mru**
- **mtu**
- **show interface brief**

show interface brief

Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show interface brief`

Mode User Exec and Privileged Exec

Output **Figure 12-4: Example output from the show interface brief command**

```
awplus#show int brief
Interface              Status          Protocol
port1.0.1              admin up        down
port1.0.2              admin up        down
port1.0.3              admin up        down
port1.0.4              admin up        down
port1.0.5              admin up        down
port1.0.6              admin up        running
lo                     admin up        running
vlan1                  admin up        down
vlan2                  admin up        down
```

Table 12-1: Parameters in the output of the show interface brief command

Parameter	Description
`Interface`	The name or type of interface.
`Status`	The administrative state. This can be either **admin up** or **admin down**.
`Protocol`	The link state. This can be either **down**, **running**, or **provisioned**.

Related Commands **show interface**
show interface memory

show interface status

Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the switch are shown.

Syntax `show interface [<port-list>] status`

Parameter	Description
`<port-list>`	The ports to display information about. The port list can be: ■ a switch port (e.g. `port1.0.6`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Examples To display the status of ports 1.0.1 to 1.0.5, use the commands:

```
awplus# show interface port1.0.1-1.0.4 status
```

Figure 12-5: Example output from the show interface <port-list> status command

```
awplus#show interface port1.0.1 -1.0.5 status
Port       Name               Status            Vlan Duplex   Speed Type
port1.0.1                     notconnect           1 auto      auto 1000BASE-T
port1.0.2                     notconnect           1 auto      auto 1000BASE-T
port1.0.3                     notconnect           1 auto      auto 1000BASE-T
port1.0.4                     notconnect           1 auto      auto 1000BASE-T
```

To display the status of all ports, use the commands:

```
awplus# show interface status
```

Figure 12-6: Example output from the show interface status command

```
awplus#sho int status
Port      Name               Status            Vlan Duplex   Speed Type
port1.0.1 Trunk_Net          connected        trunk a-full  a-1000 1000BaseTX
port1.0.2 Access_Net1        connected            5 full     100 1000BaseTX
port1.0.3 Access_Net1        disabled             5 auto      auto 1000BaseTX
port1.0.4 Access_Net2        connected            6 a-half   a-100 1000BaseTX
port1.0.5 Private_Prom       connected           10 a-full   a-100 1000BaseTX
port1.0.6 Private_Net1       connected        10,11 a-full   a-100 1000BaseTX
port1.0.7 Private_Net2       connected        10,12 a-full   a-100 1000BaseTX
port1.0.8                    notconnect           1 auto      auto 1000BaseTX
.
.
port1.0.23                   disabled             1 auto      auto not present
port1.0.24                   notconnect           1 auto      auto unknown
sa1                          notconnect       trunk auto      auto
```

Table 12-2: Parameters in the output from the show interface status command

Parameter	Description
`Port`	Name/Type of the interface.
`Name`	Description of the interface.
`Status`	The administrative and operational status of the interface; one of: ■ disabled: the interface is administratively down. ■ connect: the interface is operationally up. ■ notconnect: the interface is operationally down.
`Vlan`	VLAN type or VLAN IDs associated with the port: ■ When the VLAN mode is trunk, it displays **trunk** (it does not display the VLAN IDs). ■ When the VLAN mode is access, it displays the VLAN ID. ■ When the VLAN mode is private promiscuous, it displays the primary VLAN ID if it has one, and **promiscuous** if it does not have a VLAN ID. ■ When the VLAN mode is private host, it displays the primary and secondary VLAN IDs. ■ When the port is an Eth port, it displays **none**: there is no VLAN associated with it. ■ When the VLAN is dynamically assigned, it displays the current dynamically assigned VLAN ID (not the access VLAN ID), or **dynamic** if it has multiple VLANs dynamically assigned.
`Duplex`	The actual duplex mode of the interface, preceded by **a-** if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.
`Speed`	The actual link speed of the interface, preceded by **a-** if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.
`Type`	The type of interface, e.g. 1000BaseTX. For SFP bays, it displays **Unknown** if it does not recognize the type of SFP installed, or **Not present** if an SFP is not installed or is faulty.

Related Commands

show interface
show interface memory

shutdown

This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer.

Use the **no** variant of this command to disable this function and therefore to bring the link back up again.

Syntax

```
shutdown
no shutdown
```

Mode Interface Configuration

Example The following example shows the use of the `shutdown` command to shut down `port1.0.2`.

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

The following example shows the use of the `no shutdown` command to bring up `port1.0.2`.

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

The following example shows the use of the `shutdown` command to shut down `vlan2`.

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

The following example shows the use of the `no shutdown` command to bring up `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no shutdown
```

Chapter 13: Interface Testing Commands

Command List 13.2
clear test interface 13.2
service test 13.3
test interface 13.4

Command List

This chapter provides an alphabetical reference of commands used for testing interfaces.

clear test interface

This command clears test results and counters after issuing a test interface command. Test results and counters must be cleared to issue subsequent test interface commands later on.

Syntax `clear test interface {<port-list>|all}`

Parameter	Description
<port-list>	The ports to test. A port-list can be: ■ a switch port (e.g. `port1.0.6`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-port1.0.6` ■ a comma-separated list of the above, e.g. `port1.0.1,port1.0.5-1.0.6` The specified ports must exist.
`all`	All interfaces

Mode Privileged Exec

Examples To clear the counters for `port1.0.1` use the command:

```
awplus# clear test interface port1.0.1
```

To clear the counters for all interfaces use the command:

```
awplus# clear test interface all
```

Related Commands test interface

service test

This command puts the device into the interface testing state, ready to begin testing. After entering this command, enter Interface Configuration mode for the desired interfaces and enter the command **test interface**.

Do not test interfaces on a device that is part of a live network—disconnect the device first.

Use the **no** variant of this command to stop the test service.

Syntax

```
service test
no service test
```

Mode Global Configuration

Example To put the device into a test state, use the command:

```
awplus(config)# service test
```

Related Commands **test interface**

test interface

This command starts a test on a port or all ports or a selected range or list of ports.

Use the **no** variant of this command to disable this function. The test duration can be configured by specifying the time in minutes after specifying a port or ports to test.

For an example of all the commands required to test switch ports, see the Examples section in this command. To test the Eth port, set its speed to 100 by using the command **speed 100.**

Note Do not run test interface on live networks because this will degrade network performance.

Syntax

```
test interface {<port-list>|all} [time{<1-60>|cont}]
no test interface {<port-list>|all}
```

Parameter	Description
<port-list>	The ports to test. A port-list can be: ■ a switch port (e.g. `port1.0.6`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-port1.0.6` ■ a comma-separated list of the above, e.g. `port1.0.1,port1.0.5-1.0.6` The specified ports must exist.
`all`	All ports
`time`	Keyword entered prior to the value for the time duration of the interface test.
<1-60>	Specifies duration of time to test the interface or interfaces in minutes (from a minimum of 1 minute to a maximum of 60 minutes). The default is 4 minutes.
`cont`	Specifies continuous interface testing until canceled with command negation.

Mode Privileged Exec

Example To test the switch ports in VLAN 1, install loopbacks in the ports, and enter the following commands:

```
awplus(config)# service test
awplus(config)# no spanning-tree rstp enable bridge-forward
awplus(config)# interface vlan1
awplus(config-if)# shutdown
awplus(config-if)# end
awplus# test interface all
```

To see the output, use the commands:

```
awplus# show test
```

```
awplus# show test count
```

To start the test on all interfaces for 1 minute use the command:

```
awplus# test interface all time 1
```

Related Commands **clear test interface**

Part 2: Layer Two Switching

- Chapter 14 Switching Introduction
- Chapter 15 Switching Commands
- Chapter 16 VLAN Introduction
- Chapter 17 VLAN Commands
- Chapter 18 Spanning Tree Introduction: STP, RSTP, and MSTP
- Chapter 19 Spanning Tree Commands
- Chapter 20 Link Aggregation Introduction and Configuration
- Chapter 21 Link Aggregation Commands
- Chapter 22 Power over Ethernet Introduction
- Chapter 23 Power over Ethernet Commands

Chapter 14: Switching Introduction

Introduction 14.2
Physical Layer Information 14.3
Switch Ports 14.3
Activating and Deactivating Switch Ports 14.4
Autonegotiation 14.4
Duplex Mode 14.4
Speed Options 14.4
MDI/MDIX Connection Modes 14.5
The Layer 2 Switching Process 14.7
The Ingress Rules 14.7
The Learning Process 14.8
The Forwarding Process 14.9
The Egress Rules 14.9
Layer 2 Filtering 14.11
Ingress Filtering 14.11
Storm Control 14.12
Loop Protection 14.13
Loop Detection 14.13
Thrash Limiting 14.14
Support for Jumbo Frames 14.16
Port Mirroring 14.17
Port Security 14.18
IEEE 802.1X 14.18
Static MAC Address 14.18
Quality of Service 14.19
IGMP Snooping 14.20

Introduction

This chapter gives an overview of Layer 1 and 2 switching.

Layer 2 switches are used to connect multiple Local Area Network (LAN) segments together to form an extended LAN. Stations connected to different LANs can be configured to communicate with one another as if they were on the same LAN. They can also divide one physical LAN into multiple Virtual LANs (VLANs). Stations connected to each other on the same extended LAN can be grouped in separate VLANs, so that a station in one VLAN can communicate directly with other stations in the same VLAN, but must go through higher layer routing protocols to communicate with those stations in other VLANs.

Layer 2 switches appear transparent to higher layer protocols, transferring frames between the data link layers of the networks to which they are attached. A Layer 2 switch accesses each physical link according to the rules for that particular network. Access may not always be instant, so the switch must be capable of storing and forwarding frames.

Storing and forwarding enables the switch to examine both the VLAN tag fields and Ethernet MAC address fields in order to forward the frames to their appropriate destination. In this way, the switch can act as an intelligent filtering device, redirecting or blocking the movement of frames between networks.

Because switch ports can sometimes receive frames faster than it can forward them, the switch has Quality of Service (QoS) queues in which frames await transmission according to their priority. Such a situation could occur where data enters a number of input ports all destined for the same output port.

The switch can be used to:

- Increase both the physical extent and the maximum number of stations on a LAN. LANs are limited in their physical extent by the signal distortion and propagation delay characteristics of the media. The switch overcomes this limitation by receiving a frame on one LAN and then retransmitting it to another. The physical characteristics of the LAN media also place a practical limit on the number of stations that can be connected to a single LAN segment. The switch overcomes this limitation by joining LAN segments to form an extended LAN capable of supporting more stations than either of the individual LAN segments.
- Connect LANs that have a common data link layer protocol but different physical media, for example, Ethernet 10BASET, 100BASET, and 10BASEF.
- Increase the availability of LANs by allowing multiple redundant paths to be physically configured and selected dynamically, using the Spanning Tree algorithm.
- Reduce the load on a LAN or increase the effective bandwidth of a LAN, by filtering traffic.
- Prioritize the transmission of data with high Quality of Service requirements.

By using Virtual LANs (VLANs), a single physical LAN can be separated into multiple Virtual LANs. VLANs can be used to:

- Further improve LAN performance, as broadcast traffic is limited to LAN segments serving members of the VLAN to which the sender belongs.
- Provide security, as frames are forwarded to those stations belonging to the sender's VLAN, and not to stations in other VLANs on the same physical LAN.
- Reduce the cost of moving or adding stations to function or security based LANs, as this generally requires only a change in the VLAN configuration.

Physical Layer Information

Switch Ports

A unique port number identifies each switch port. The software supports a number of features at the physical level that allow it to be connected in a variety of physical networks. This physical layer (Layer 1) versatility includes:

- Enabling and disabling of ports
- Auto negotiation of port speed and duplex mode, where supported by the port type
- Manual setting of port speed and duplex mode, where supported by the port type
- Link up and link down triggers
- Packet storm protection
- Port mirroring
- Support for SNMP management

Port numbering

Ports are numbered using a 3 digit format `x.y.z` where `x` is the device number (within a stacked configuration), `y` is the module number within the device, and `z` is the port number within the module. Ports connected directly to the switch chassis or baseboard (rather than a pluggable module) are given the module number `0`. In an unstacked configuration all device numbers are `1`. For example, `port1.2.6` represents device `1`, module `2`, port `6`.

Adding a description

You can add a description to an interface to help identify its purpose or position. For example, to add the description "connected to Nerv" to `port1.0.3`, use the commands:

```
awplus(config)# interface port1.0.3
awplus(config-if)# description connected to Nerv
```

Port ranges

Continuous

To configure a continuous range of ports at the same time, enter the range in the format:

`portx.y.z-portx.y.z`

For example, to configure the same interface setting on `port1.0.1` to `port1.0.2`, enter the Global Configuration mode command:

```
awplus(config)# interface port1.0.1-port1.0.2
```

Non-continuous

To configure a non-continuous set of ports at the same time, enter a comma-separated list:

`portx.y.z,portx.y.z`

For example, to configure the same interface setting on `port1.0.1` and `port1.0.5`, enter the Global Configuration mode command:

```
awplus(config)# interface port1.0.1,port1.0.5
```

You can combine a hyphen-separated range and a comma-separated list. To configure the same setting on `port1.0.1` to `port1.0.3` and `port1.0.5`, enter the Global Configuration mode command:

```
awplus(config)# interface port1.0.1-port1.0.3,port1.0.5
```

Activating and Deactivating Switch Ports

An active switch port is one that is available for packet reception and transmission. Disabling a switch port does not affect the STP operation on the port. By default ports and VLANs are activated.

To shutdown a port or VLAN use the **shutdown** command on page 12.15. Use the **no** variant of this command to reactivate it.

Autonegotiation

Autonegotiation lets the port adjust its speed and duplex mode to accommodate the device connected to it. When the port connects to another autonegotiating device, they negotiate the highest possible speed and duplex mode for both of them.

By default, all ports autonegotiate. Setting the port to a fixed speed and duplex mode may be necessary when connecting to a device that cannot autonegotiate.

Duplex Mode

Ports can operate in full duplex or half duplex mode depending on the type of port it is. When in full duplex mode, a port transmits and receives data simultaneously. When in half duplex mode, the port transmits or receives but not both at the same time.

You can set a port to use either of these options, or allow it to autonegotiate the duplex mode with the device at the other end of the link. To configure the duplex mode, use these commands:

`awplus#` `configure terminal`	Enter Global Configuration mode
`awplus(config)#` `interface port1.0.1`	Enter Interface Configuration mode for port 1.0.1
`awplus(config-if)#` `duplex {auto|full|half}`	Enter the Duplex mode for port 1.0.1

Speed Options

Before configuring a port's speed, check the hardware limit for the particular port type. The following list can be used as a guide:

- non-SFP RJ-45 copper switch ports: 10, 100 or 1000 Mbps
- supported tri-speed copper SFPs: 10, 100 or 1000 Mbps
- fiber SFPs: 100 Mbps to 1000 Mbps, depending on the SFP type
- SFP+ / XFP modules: 10 Gbps

For the latest list of approved SFP transceivers either contact your authorized distributor or reseller, or visit **alliedtelesis.com**.

You can set a port to use one of these speed options, or allow it to autonegotiate the speed with the device at the other end of the link.

Most types of switch port can operate in either full duplex or half duplex mode. In full duplex mode a port can transmit and receive data simultaneously. In half duplex mode the port can either transmit or receive, but not at the same time.

Make sure that the configuration of the switch matches the configuration of the device at the far end of the link. In particular, avoid having one end autonegotiate duplex mode while the other end is fixed. For example, if you set one end of a link to autonegotiate and fix the other end at full duplex, the autonegotiating end cannot determine that the fixed end is full duplex capable. Therefore, the autonegotiating end selects half-duplex operation. This results in a duplex mismatch and packet loss. To avoid this, either fix the mode at both ends, or use autonegotiation at both ends.

Configuring the port speed

To set the port speed to 1000 Mbps on port 1.0.1, use the commands:

`awplus#`	
`configure terminal`	Enter the Global Configuration mode.
`awplus(config)#`	
`interface port1.0.1`	Enter Interface Configuration mode for port 1.0.1
`awplus(config-if)#`	
`speed 1000`	Set the port speed for port 1.0.1 to 1000 Mbps.

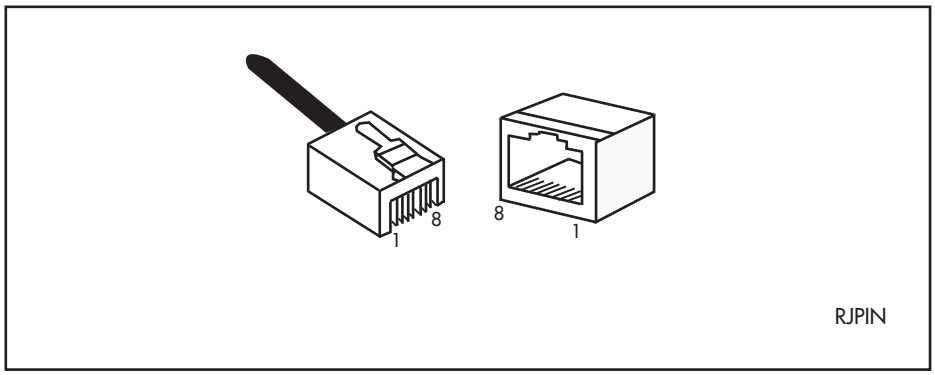
MDI/MDIX Connection Modes

By default, copper 10Base-T, 100Base-T, and 1000Base-T ports on the switch automatically set the Media Dependant Interface mode to MDI or MDIX for successful physical connections. We recommend using this default setting. However, you can configure them to have either fixed MDI mode or fixed MDIX mode by using the **polarity** command on page 15.24. MDI/MDIX mode polarity does not apply to fiber ports.

Connections to 10BASE-T, 100BASE-T, and 1000BASE-T networks may either be straight though (MDI) or crossover (MDIX). The crossover connection can be achieved by using either a crossover cable or by integrating the crossover function within the device. In the latter situation, the connector is referred to as an MDIX connection. Refer to your switch's Hardware Reference for more detailed information on physical connections cabling.

The IEEE 802.3 standard defines a series of Media Dependant Interface types and their physical connections. For twisted pair (10BASE-T) networking, the standard defines that connectors that conform to the IEC 60603-7 standard. The **Figure 14-1**f shows a connector of this type.

Figure 14-1: Connector used for 10BASE-T networks



The Layer 2 Switching Process

The Layer 2 switching process comprises these related but separate processes:

- **The Ingress Rules**
- **The Learning Process**
- **The Forwarding Process**
- **The Egress Rules**

Ingress rules admit or discard frames based on their VLAN tagging.

The Learning process learns the MAC addresses and VLAN membership of frames admitted on each port.

The Forwarding process determines which ports the frames are forwarded to, and the Quality of Service priority with which they are transmitted.

Finally, Egress rules determine for each frame whether VLAN tags are included in the Ethernet frames that are transmitted.

These processes assume that each station on the extended LAN has a unique data link layer address, and that all data link layer frames have a header which includes the source (sender's) MAC address and destination (recipient's) MAC address.

The Ingress Rules

All frames, tagged and untagged, that a VLAN-aware switch receives must be classified into a VLAN. Each received frame is mapped to exactly one VLAN. If an incoming frame is tagged with a valid VLAN identifier (VID) then that VID is used. If an incoming frame is untagged or is priority tagged (a tagged frame with a VID of all zeros), then the switch uses internal VLAN association rules to determine the VLAN it belongs to. The default settings for the ingress rules are to Admit All Frames, and for Ingress Filtering to be on.

Every port belongs to one or more VLANs so every incoming frame has a VID to show which VLAN it belongs. The final part of the Ingress Rules depends on whether Ingress Filtering is enabled for the port. If Ingress Filtering is disabled, all frames are passed on to the Learning process, regardless of which VLAN they belong to. If Ingress Filtering is enabled (by default), frames are admitted only when they have the VID of a VLAN to which the port belongs. Frames are discarded when they do not have an associated VID matching the VLAN assigned to a port.

The possible association rules, in order of precedence, are:

- IP subnet/IPX network classification
- protocol classification
- port classification

The default VLAN classification is based upon the port on which the incoming frame (untagged, or priority tagged) was received. It is possible for an incoming untagged, or priority tagged, frame to match more than one of the association rules.

Each port on the switch can be configured to be one of two modes:

- only untagged frames - access mode
- VLAN-tagged frames - trunk mode

Access mode

This mode can be used to connect to VLAN unaware devices. Frames to and from access mode ports carry no VLAN tagging information.

Trunk mode

This mode is used to connect VLAN capable devices. All devices that connect using trunk mode ports must be VLAN aware.

You can specify a "native" VLAN on a trunk port. When the port receives untagged packets, it will tag the packets with the VID of the native VLAN. Note that packets from the native VLAN egress the port untagged.

To specify the native VLAN, use the **switchport trunk native vlan** command on page 17.28.

The Learning Process

The learning process uses an adaptive learning algorithm, sometimes called ***backward learning***, to discover the location of each station on the extended LAN.

All frames admitted by the ingress rules on any port are passed on to the forwarding process when they are for destinations in the same VLAN. Frames destined for other VLANs are passed to a Layer 3 protocol, such as IP. For every frame admitted, the frame's source MAC address and VID are compared with entries in the forwarding database for the VLAN (also known as a ***MAC Address table***) maintained by the switch. When the frame's source address is not in the forwarding database for the VLAN, the address is added and an ageing timer for that entry is started. When the frame's source address is already in the forwarding database, the ageing timer for that entry is restarted.

By default, switch learning is enabled. It can be disabled with the **no mac address-table acquire** command, and re-enabled using the **mac address-table acquire** command on page 15.16.

If the ageing timer for an entry in the forwarding database expires before another frame with the same source address is received, the entry is removed from the forwarding database. This prevents the forwarding database from being filled with information about stations that are inactive or have been disconnected from the network. It also ensures that entries for active stations are kept alive in the forwarding database.

By default, the ageing timer is enabled with a default ageing-time. The ageing timer can be reset to the default with the **no mac address-table ageing-time** command. The ageing timer can be increased or decreased using the **mac address-table ageing-time** command.

If switch learning is disabled and the ageing timer has aged out all dynamically learned filter entries, only statically entered MAC source addresses decide the packets to forward or discard. When the switch finds no matching entries in the forwarding database during the forwarding process, all switch ports in the VLAN are flooded with the packet, except the port that received it.

The default for the mac address-table ageing-time is 300 seconds (5 minutes) and can be modified by using the command **mac address-table ageing-time**. The **no mac address-table ageing-time** command will reset the ageing-time back to the default (5 minutes).

To set the mac address-table ageing-time to 1000 seconds:

`awplus#`	
`configure terminal`	Enter the config terminal mode
`awplus(config)#`	
`mac address-table ageing-time 1000`	Set the ageing time to 1000 seconds

To display general switch settings, including settings for switch learning and the switch ageing timer, use the **show system** command on page 8.46.

The Forwarding Process

After a VID is assigned to a frame using the ingress rules, the switch forwards it to the destination MAC address specified in the frame. To do this the switch must learn which MAC addresses are available on each port for each VLAN. When the destination MAC address is not found, the switch floods the frame on all ports that are members of the VLAN except the port on which the frame was received.

The forwarding database (also known as the ***MAC Address table***) determines the egress port on which the destination MAC address has been learned. MAC addresses are learned dynamically as part of the Layer 2 switching process.

The forwarding database is ordered according to MAC address and VLAN identifier. This means a MAC address can appear more than once in the forwarding database having been learned on the same port but for different VLANs. This could occur if the IP address of an end station is changed thereby moving the end station to a different IP subnet-based VLAN while still connected to the same switch port. When the forwarding database ageing process is enabled, old entries in the forwarding database are deleted after a user-configurable period.

If the destination address is found, the switch discards the frame when the port is not in the STP forwarding or disabled state if the destination address is on the same port as the source address, or if there is a static filter entry for the destination address set to **discard** (see **"Layer 2 Filtering" on page 14.11**). Otherwise, the frame is forwarded on the indicated port.

Forwarding occurs only when the port on which the frame was received is in the Spanning Tree forwarding or disabled state. The destination address is then looked up in the forwarding database for the VLAN.

The Egress Rules

After the forwarding process has determined from which ports and transmission queues to forward a frame, the egress rules for each port determine whether the outgoing frame is VLAN-tagged with its numerical VLAN identifier (VID).

A port must belong to a VLAN at all times unless the port has been set as the mirror port for the switch.

A port can transmit VLAN-tagged frames for any VLAN to which the port belongs. A port can transmit untagged frames for any VLAN for which the port is configured, e.g. IP subnet-based or protocol-based, unless prevented by the port-based VLAN egress rules. A port that belongs to a port-based VLAN can transmit untagged packets for only one VLAN. For more information about VLANs and VLAN tagging, see **Chapter 16, VLAN Introduction**.

For more information on port tagging see the following commands:

switchport mode access command on page 17.16

switchport mode trunk command on page 17.22

Layer 2 Filtering

The switch has a forwarding database (also known as the ***MAC address table***) whose entries determine whether frames are forwarded or discarded over each port. Entries in the forwarding database are created dynamically by the learning process. A dynamic entry is automatically deleted from the forwarding database when its ageing timer expires.

The forwarding database supports queries by the forwarding process as to whether frames with given values of the destination MAC address field should be forwarded to a given port.

For each VLAN, the destination MAC address of a frame to be forwarded is checked against the forwarding database. If there is no entry for the destination address and VLAN, the frame is transmitted on all ports in the VLAN that are in the forwarding state, except the port on which the frame was received. This process is referred to as ***flooding***. If an entry is found in the forwarding database but the entry is not marked ***forwarding*** or the entry points to the same port the frame was received on, the frame is discarded. Otherwise, the frame is transmitted on the port specified by the forwarding database.

Ingress Filtering

The **ingress-filter** parameter of the **switchport mode trunk** command on page 17.22 and the **switchport mode access** command on page 17.16, enables or disables ingress filtering of frames entering the specified port (or port range).

Each port on the switch belongs to one or more VLANs. If ingress filtering is enabled, any frame received on the specified port is only admitted if its VID matches one for which the port is tagged. Any frame received on the port is discarded if its VID does not match one for which the port is tagged.

Untagged frames are admitted and are assigned the VLAN Identifier (VID) of the port's native VLAN. Ingress filtering can be turned off by setting the **disable** parameter of the above two commands. The default setting of the **enable** / **disable** parameter option is **enable**.

Note

Enabling the **vlan-disable** parameter of the **thrash-limiting** command on page 15.46 will also enable ingress filtering, and will override the setting of the switchport mode access, and trunk commands

Storm Control

The packet storm-control feature enables you to set limits on the reception rate of broadcast, multicast frames and destination lookup failures. You can set separate limits beyond which each of the different packet types are discarded.

Note A destination lookup failure (DLF) is the event of receiving a unicast Ethernet frame with an unknown destination address.

For more information on applying storm-control, see the **storm-control level** command on page 15.45.

To apply storm-control by limiting broadcasts to 30% on `port1.0.4`:

`awplus(config-if)#` `configure terminal`	Enter Global Configuration mode.
`awplus(config-if)#` `interface port1.0.4`	Enter the Interface Configuration mode for the selected port.
`awplus(config-if)#` `storm-control broadcast level 30`	Configure the interface.

To turn off storm protection on `port1.0.4`:

`awplus(config-if)#` `configure terminal`	Enter Global Configuration mode.
`awplus(config-if)#` `interface port1.0.4`	Enter the Interface Configuration mode for the selected port.
`awplus(config-if)#` `no storm-control broadcast level`	Configure the interface.

Loop Protection

Loop protection is a general term that embraces several different methods you can apply to protect your network from effects such as broadcast storms that can result from data loops or equipment malfunction.

Two methods of loop protection are available:

- **Loop Detection**
- **Thrash Limiting**

Loop Detection

Introduction

This feature is used to detect loops with a network segment. If a loop is detected then a selected protection mechanism is applied to limit the effect of the loop. The loop protection actions can be applied either to the port at which the loop is detected or to the VLAN within which the loop was detected.

Limiting Actions

You can configure loop detection to apply one of the following mechanisms when a loop condition is detected:

- Block all traffic on the port (or aggregated link) that detected the loop, and take **down** the link.
- Block all traffic on the port (or aggregated link) that detected the loop, but keep the link in the **up** state.
- Block all traffic on a vlan. Note that setting this parameter will also enable ingress filtering. This is the default action.
- Take no action, but log the details.
- Take no action.

Operation

To detect loops this feature operates by transmitting a series of Loop Detection Frames (LDFs) from each switch port out into the network. If no loops exist, then none of these frame should ever return. If a frame returns to its original port, the detection mechanism assumes that there is a loop somewhere in the network and offers a number of protective options.

Each LDF is a Layer 2 LLC frame that contains the following components:

- the source MAC address of the originating switch
- the destination MAC address of the non-existent end station 00-00-F4-27-71-01
- VLAN ID (where the port is a tagged member of a VLAN).
- a randomly generated LDF ID number.

You can set the detection mechanism to remember the LDF ID of up to 5 of the most recently transmitted LDF frames. Each of the 5 most recently transmitted frames is compared with every frame that arrives at that same port.

Configuration

To enable loop protection and configure its basic parameters, you use the **loop-protection** command on page 15.12.

Example To enable the loop-detect mechanism, and generate loop-detect frames once every 5 seconds, use the command:

```
awplus(config)# loop-protection loop-detect ldf-interval 5
```

Note LDFs are sent sequentially for each VLAN defined to a particular port. For example, if a particular port in this example is a member of 4 VLANs, then the LDFs will be sent from this port at the rate of 4 frames every 5 seconds.

You can now use the **loop-protection action** command on page 15.13 configure the action that the switch will take if a loop is detected.

Example To disable an interface, and bring the link down, when a network loop is detected, use the command:

```
awplus(config-if)# loop-protection action link-down
```

Now decide how long you want the protective action to apply for. You configure this function by using the **loop-protection timeout** command on page 15.15.

Example To configure a loop protection action timeout of 10 seconds, use the command:

```
awplus(config-if)# loop-protection timeout 10
```

Example To configure a loop protection action delay time of 10 seconds, use the commands:

```
awplus(config-if)# loop-protection action-delay-time
                   10
```

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:** MAC 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 on page 12.15.
- **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 on page 15.46:

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

Support for Jumbo Frames

Jumbo frames are frames with more than 1500 bytes of payload. You can enable jumbo frame support on the switch to improve throughput and network utilization. Jumbo frame support allows you to put more data in each packet that the switch has to process.

The maximum received packet size is 16357 bytes.

You can increase the Maximum Receive Unit (MRU) size for switch ports to receive jumbo frames with payload larger than 1500 bytes. To increase MRU size, use the **mru** command on page 12.5.

Note

Jumbo packet switching is supported for L2 and L3 traffic flows that have established traffic paths. Jumbo frames cannot be used for establishing these network paths. Please use frames less than 1518 bytes to establish the path, for example by pinging the destination.

Port Mirroring

Port mirroring enables traffic being received and transmitted on a switch port to be sent to another switch port, the mirror port, usually for the purposes of capturing the data with a protocol analyzer.

The mirror port is the only switch port that does not belong to a VLAN, and therefore does not participate in any other switching. Before the mirror port can be set, it must be removed from all trunk groups and all VLANs except the default VLAN.

The following example sets mirroring on ports 1.0.2 and 1.0.5 for both incoming and outgoing data.

Note

Due to the internal hardware properties of the switch, frames that are destined to leave the mirrored port untagged (i.e. will have their VLAN tag removed on egress) will be received by the mirror port with the tag retained. Consequently, if frames were being transmitted by the mirror port (into the network) at wire speed, then the mirror port might be unable to accept all the frames supplied to it.

To configure port 1.0.2 to mirror port 1.0.5:

`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `interface port1.0.2`	Enter the Interface Configuration mode for port1.0.2.
`awplus(config-if)#` `mirror interface port1.0.5 direction both`	Configure this port to mirror port 1.0.5.

Port Security

The port security features provide control over the stations connected to each switch port.

- 802.1x
- Static MAC address

IEEE 802.1X

IEEE 802.1X restricts unauthenticated devices from connecting to the switch. After authentication is successful, traffic is allowed through the switch. For more information see **Chapter 46, 802.1X Introduction and Configuration**.

Static MAC Address

If a new MAC address is seen on a port with port security enabled and the MAC address is statically configured for another port, a violation is triggered. The maximum learn limit will be ignored and the specified intrusion action for the port will be carried out.

Quality of Service

Quality of Service (QoS) enables you to both prioritize traffic and limit its available bandwidth. The concept of QoS is a departure from the original networking protocols, in which all traffic on the Internet or within a LAN had the same available bandwidth. Without QoS, all traffic types are equally likely to be dropped if a link becomes oversubscribed. This approach is now inadequate in many networks, because traffic levels have increased and networks often carry time-critical applications such as streams of real-time video data. QoS also enables service providers to easily supply different customers with different amounts of bandwidth.

Configuring Quality of Service involves two separate stages:

1. Classifying traffic into flows, according to a wide range of criteria. Classification is performed by the switch's class maps.

2. Acting on these traffic flows.

For more information on QoS see **Chapter 40, Quality of Service (QoS) Introduction** and **Chapter 41, QoS Commands**.

IGMP Snooping

IGMP (Internet Group Management Protocol) is used by IP hosts to report their multicast group memberships to routers and switches. IP hosts join a multicast group to receive broadcast messages directed to the multicast group address. IGMP is an IP-based protocol and uses IP addresses to identify both the multicast groups and the host members. For a VLAN-aware devices, this means multicast group membership is on a per-VLAN basis. If at least one port in the VLAN is a member of a multicast group, by default multicast packets will be flooded onto all ports in the VLAN.

IGMP snooping enables the switch to forward multicast traffic intelligently on the switch. The switch listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

IGMP snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will forward traffic only from those ports with multicast listeners, therefore it will not act as a simple hub and flood all multicast traffic out all ports. IGMP snooping is independent of the IGMP and Layer 3 configuration, so an IP interface does not have to be attached to the VLAN, and IGMP does not have to be enabled or configured.

IGMP snooping is enabled by default.

For more information on IGMP see **Chapter 32, IGMP Snooping Introduction** and **Chapter 33, IGMP Snooping Commands**.

Chapter 15: Switching Commands

Command List 15.2
backpressure 15.2
clear loop-protection counters 15.3
clear mac address-table static 15.4
clear mac address-table dynamic 15.5
clear port counter 15.7
duplex 15.8
flowcontrol (switch port) 15.9
linkflap action 15.11
loop-protection 15.12
loop-protection action 15.13
loop-protection action-delay-time 15.14
loop-protection timeout 15.15
mac address-table acquire 15.16
mac address-table ageing-time 15.17
mac address-table static 15.18
mac address-table thrash-limit 15.19
mirror interface 15.20
platform stop-unreg-mc-flooding 15.22
polarity 15.24
show flowcontrol interface 15.25
show loop-protection 15.26
show mac address-table 15.27
show mac address-table thrash-limit 15.29
show mirror 15.30
show mirror interface 15.31
show platform 15.32
show platform classifier statistics utilization brief 15.33
show platform port 15.34
show port-security interface 15.40
show port-security intrusion 15.41
show storm-control 15.42
speed 15.43
storm-control level 15.45
thrash-limiting 15.46

Command List

This chapter provides an alphabetical reference of commands used to configure switching. For more information see **Chapter 14, Switching Introduction**.

backpressure

This command provides a method of applying flow control to ports running in half duplex mode. The setting will only apply when the link is in the half-duplex state.

You can disable backpressure on an interface using the **off** parameter or the **no** variant of this command.

Syntax

```
backpressure {on|off}
no backpressure
```

Parameters	Description
`on`	Enables half-duplex flow control.
`off`	Disables half-duplex flow control.

Default Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; **backpressure on** is shown for interfaces if this feature is enabled.

Mode Interface Configuration

Usage The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Back pressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the **flowcontrol (switch port)** command on page 15.9 operates only on full-duplex links, whereas back pressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the switch will simulate a collision by transmitting a CSMACD jamming signal from this port until the buffer empties. The jamming signal causes the sending switch to stop transmitting and wait a random period of time, before retransmitting its data, thus providing time for the buffer to clear. Although this command is only valid for switch ports operating in half-duplex mode the remote switch (the one sending the data) can be operating in the full duplex mode.

To see the currently-negotiated duplex mode for ports whose links are up, use the command **show interface**. To see the configured duplex mode (when different from the default), use the command **show running-config**.

Examples To enable back pressure flow control on interfaces `port1.0.1-port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# backpressure on
```

To disable back pressure flow control on interface `port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# backpressure off
```

Validation Commands **show running-config**
show interface

Related Commands **duplex**

clear loop-protection counters

Use this command to clear the counters for the Loop Protection counters.

Syntax

```
clear loop-protection [interface <port-list>] counters
```

Parameters	Description
`interface`	The interface whose counters are to be cleared.
<port-list>	A port, a port range, or an aggregated link.

Mode Privileged Exec

Examples To clear the counter information:

```
awplus# clear loop-protection counters
awplus# clear loop-protection interface port1.0.1 counters
```

clear mac address-table static

Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

Syntax

```
clear mac address-table static [address <mac-address>|
   interface <port>|vlan <vid>]
```

Parameter	Description
`address`	Specify a MAC (Media Access Control) address to be cleared from the filtering database.
<mac-address>	Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.
`interface`	Specify a switch port to be cleared from the filtering database.
<port>	Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
`vlan`	Specify a VLAN to be cleared from the filtering database.
<vid>	Enter a VID (VLAN ID) in the range `<1-4094>` to be cleared from the filtering database.

Mode Privileged Exec

Usage Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with **clear mac address-table dynamic** command on page 15.5.

Examples This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a given interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries filtering database entries configured through the CLI for a given mac address.

```
awplus# clear mac address-table static address 0202.0202.0202
```

Related Commands
clear mac address-table dynamic
mac address-table static
show mac address-table

clear mac address-table dynamic

Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface or a VLAN interface.

Syntax

```
clear mac address-table dynamic [address <mac-address>|
   interface <port> [instance <inst>]|vlan <vid>]
```

Parameter	Description
`interface`	Specify a switch port to be cleared from the filtering database.
<port>	Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
`address`	Specify a MAC (Media Access Control) address to be cleared from the filtering database.
<mac-address>	Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.
`instance`	Specify an MSTP (Multiple Spanning Tree) instance to be cleared from the filtering database.
<inst>	Enter an MSTP instance in the range `<1-63>` to be cleared from the filtering database.
`vlan`	Specify a VLAN to be cleared from the filtering database.
<vid>	Enter a VID (VLAN ID) in the range `<1-4094>` to be cleared from the filtering database.

Mode Privileged Exec

Usage Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

Use the optional `instance` parameter to clear the filtering database entries associated with a specified MSTP instance Note that you must first specify a switch port interface before you can specify an MSTP instance.

Compare this usage and operation with the **clear mac address-table static** command on page 15.4. Note that an MSTP instance cannot be specified with **clear mac address-table static**.

Examples This example shows how to clear all dynamically learned filtering database entries for all interfaces, addresses, VLANs.

```
awplus# clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through switch operation for a given MAC address.

```
awplus# clear mac address-table dynamic address 0202.0202.0202
```

This example shows how to clear all dynamically learned filtering database entries when learned through switch operation for a given MSTP instance `1` on switch port interface `port1.0.2`.

```
awplus# clear mac address-table dynamic interface port1.0.2
        instance 1
```

Related Commands

clear mac address-table static
show mac address-table

clear port counter

Use this command to clear the packet counters of the port.

Syntax `clear port counter [<port>]`

Parameter	Description
<port>	The port number or range

Mode Privileged Exec

Example To clear the packet counter for `port1.0.1`, use the command:

```
awplus#  clear port counter port1.0.1
```

Related Commands **show platform port**

duplex

This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command **show interface**. To see the configured duplex mode (when different from the default), use the command **show running-config**.

Syntax `duplex {auto|full|half}`

Parameter	Description
`auto`	Auto-negotiate duplex mode.
`full`	Operate in full duplex mode only.
`half`	Operate in half duplex mode only.

Default By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

Mode Interface Configuration

Usage Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the duplex mode of all the switch ports in the channel group by applying this command to the channel group.

Examples To specify full duplex for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

Related Commands
backpressure
polarity
speed
show interface

flowcontrol (switch port)

Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the **no** variant of this command to disable flow control for the specified switch port.

Syntax

```
flowcontrol {send|receive} {off|on}
no flowcontrol
```

Parameter	Description
`receive`	When the port receives pause frames, it temporarily stops (pauses) sending traffic.
`on`	Enable the specified flow control.
`off`	Disable the specified flow control.
`send`	When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic.

Default By default, flow control is disabled.

Mode Interface Configuration

Usage The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

Flow control is not recommended when running QoS or ACLs, because the complex queuing, scheduling, and filtering configured by QoS or ACLs may be slowed by applying flow control.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related **backpressure** command on page 15.2.

For flow control on async serial (console) ports, see the **flowcontrol hardware (asyn/console)** command on page 5.11.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
```

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive off
```

Validation Commands **show running-config**

Related Commands **backpressure**

linkflap action

Use this command to detect flapping on all ports. If more than 15 flaps occur in less than 15 seconds the flapping port will shut down.

Use the **no** variant of this command to disable flapping detection at this rate.

Syntax

```
linkflap action [shutdown]
no linkflap action
```

Parameter	Description
`linkflap`	Global setting for link flapping.
`action`	Specify the action for port.
`shutdown`	Shutdown the port.

Default Linkflap action is disabled by default.

Mode Global Configuration

Example To enable the linkflap action command on the switch, use the following commands:

```
awplus# configure terminal
awplus(config)# linkflap action shutdown
```

loop-protection

Use this command to enable the loop-protection loop-detection feature, and configure the detection mechanism parameters.

Use the **no** variant of this command to disable the loop-protection loop-detection feature.

Syntax

```
loop-protection loop-detect [ldf-interval <period>]
    [ldf-rx-window <frames>] [fast-block]

no loop-protection [loop-detect]
```

Parameter	Description
`loop-detect`	Enables loop detection when used with loop-protection keywords. Disables loop detection when used with no loop-protection keywords.
`ldf-interval`	The time (in seconds) between successive loop-detect frames being sent.
<period>	Specify a period between 1 and 600 seconds. The default is 10 seconds.
`ldf-rx-window`	The number of transmitted loop detection frames whose details are held for comparing with frames arriving at the same port.
<frames>	Specify a value for the window size between 1 and 5 frames. The default is 3 frames.
`[fast-block]`	The fast-block blocks transmitting port to keep partial connectivity.

Default The loop-protection loop-detection feature is disabled by default. The default interval is 10 seconds, and the default window size is 3 frames.

Mode Global Configuration

Usage See the **Loop Protection** section in **Chapter 14, Switching Introduction** for relevant conceptual, configuration, and overview information prior to applying this command.

Example To enable the loop-detect mechanism on the switch, and generate loop-detect frames once every 5 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# loop-protection loop-detect ldf-interval 5
```

Related Commands

loop-protection action
loop-protection timeout
show loop-protection
thrash-limiting

loop-protection action

Use this command to specify the protective action to apply when a network loop is detected on an interface.

Use the **no** variant of this command to reset the loop protection actions to the default action, vlan-disable, on an interface.

Syntax

```
loop-protection action {link-down|log-only|port-disable|vlan-disable|
   none}
no loop-protection action
```

Parameter	Description
`link-down`	Block all traffic on a port (or aggregated link) that detected the loop, and take **down** the link.
`log-only`	Details of loop conditions are logged. No action is applied to the port (or aggregated link).
`port-disable`	Block all traffic on interface for which the loop occurred, but keep the link in the **up** state.
`vlan-disable`	Block all traffic for the VLAN on which the loop traffic was detected. Note that setting this parameter will also enable ingress filtering. This is the default action.
`none`	Applies no protective action.

Default loop-protection action vlan-disable

Mode Interface Configuration

Usage See the **Loop Protection** section in **Chapter 14, Switching Introduction** for relevant conceptual, configuration, and overview information prior to applying this command.

Example To disable an interface (`port1.0.4`), and bring the link down, when a network loop is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action link-down
```

Related Commands

loop-protection
loop-protection timeout
show loop-protection
thrash-limiting

loop-protection action-delay-time

Use this command to sets the loop protection action delay time for an interface to specified values in seconds. The action delay time specifies the waiting period for the action.

Use the **no** variant of this command to reset the loop protection action delay time for an interface to default.

Syntax

```
loop-protection action-delay-time <0-86400>
no loop-protection action
```

Parameter	Description
<0-86400>	Time in seconds; 0 means action delay timer is disabled.

Default Action delay timer is disabled by default.

Mode Interface Configuration

Example To configure a loop protection action delay time of 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action-delay-time
10
```

To reset the Loop Protection action delay time to default, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no loop-protection action-delay-
time
```

Related Commands **show loop-protection**

loop-protection timeout

Use this command to specify the Loop Protection recovery action duration on an interface.

Use the **no** variant of this command to set the loop protection timeout to the default.

Syntax

```
loop-protection timeout <duration>
no loop-protection timeout
```

Parameter	Description
<duration>	The time (in seconds) for which the configured action will apply before being disabled. This duration can be set between 0 and 86400 seconds (24 hours). The set of 0 means infinity so timeout does not expire.

Default The default is 7 seconds.

Mode Interface Configuration

Usage See the **Loop Protection** section in **Chapter 14, Switching Introduction** for relevant conceptual, configuration, and overview information prior to applying this command.

Example To configure a loop protection action timeout of 10 seconds for `port1.0.4`, use the command:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection timeout 10
```

Related Commands

loop-protection
loop-protection action
show loop-protection
thrash-limiting

mac address-table acquire

Use this command to enable MAC address learning on the device.

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

Syntax

```
mac address-table acquire
no mac address-table acquire
```

Default Learning is enabled by default for all instances.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# mac address-table acquire
```

mac address-table ageing-time

Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist for at least the specified time.

The **no** variant of this command will reset the ageing-out time back to the default of 300 seconds (5 minutes).

Syntax

```
mac address-table ageing-time <ageing-timer> none
no mac address-table ageing-time
```

Parameter	Description
<ageing-timer>	*<10-1000000>* The number of seconds of persistence.
none	Disable learned MAC address timeout.

Default The default ageing time is 300 seconds.

Mode Global Configuration

Examples The following commands specify various ageing timeouts on the switch:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000

awplus# configure terminal
awplus(config)# mac address-table ageing-time none

awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

mac address-table static

Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

Syntax

```
mac address-table static <mac-addr> {forward|discard} interface
   <port> [vlan <vid>]

no mac address-table static <mac-addr> {forward|discard} interface
   <port> [vlan <vid>]
```

Parameter	Description
<mac-addr>	The destination MAC address in `HHHH.HHHH.HHHH` format.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
<vid>	The VLAN ID. If you do not specify a VLAN, its value defaults to vlan 1.

Mode Global Configuration

Usage The **mac address-table static** command is only applicable to Layer 2 switched traffic within a single VLAN. Do not apply the **mac address-table static** command to Layer 3 switched traffic passing from one VLAN to another VLAN. Frames will not be discarded across VLANs because packets are routed across VLANs. This command only works on Layer 2 traffic.

Example

```
awplus# configure terminal

awplus(config)# mac address-table static 2222.2222.2222 forward
                interface port1.0.4 vlan 3
```

Related Commands **clear mac address-table static**
show mac address-table

mac address-table thrash-limit

Use this command to set the thrash limit on the switch or stack. Thrashing occurs when a MAC address table rapidly "flips" its mapping of a single MAC address between two subnets, usually as a result of a network loop.

Use the **no** variant of this command to disable thrash limiting.

Syntax

```
mac address-table thrash-limit <rate>
no mac address-table thrash-limit
```

Parameter	Description
<rate>	sets the maximum thrash rate at which limiting is applied. This rate can be set between 5 and 255 MAC thrashing flips per second. Once the thrash limit rate is reached, the port is considered to be thrashing.

Default No thrash limiting

Mode Global Configuration

Usage Use this command to limit thrashing on the selected port range.

Example To apply a thrash limit of 100 MAC address flips per second:

```
awplus# configure terminal
awplus(config)# mac address-table thrash-limit 100
```

Related Commands **show mac address-table thrash-limit**

mirror interface

Use this command to define a mirror port and mirrored (monitored) ports and direction of traffic to be mirrored. The port for which you enter interface mode will be the mirror port.

The destination port is removed from all VLANs, and no longer participates in other switching.

Use the **no** variant of this command to disable port mirroring by the destination port on the specified source port.

Use the **none** variant of this command when using copy-to-mirror ACL and QoS commands.

Syntax

```
mirror interface <source-port-list> direction {both|receive|transmit}
mirror interface none
no mirror interface <source-port-list>
no mirror interface none
```

Parameter	Description
<source-port-list>	The source switch ports to mirror. A port-list can be: ■ a port (e.g. `port1.0.2`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.2` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6` The source port list cannot include dynamic or static channel groups (link aggregators).
`direction`	Specifies whether to mirror traffic that the source port receives, transmits, or both.
`both`	Mirroring traffic both received and transmitted by the source port.
`receive`	Mirroring traffic received by the source port.
`transmit`	Mirroring traffic transmitted by the source port.
`none`	Specify this parameter for use with the ACL (Access Control List) **access-list** and QoS (Quality of Service) default action commands when used with the **copy-to-mirror** parameter option, so you can specify the destination port (the analyzer port) for the traffic without specifying a source mirror port. See the ACL commands **access-list (hardware IP numbered)** and **access-list (hardware MAC numbered)**, and the QoS command **default-action** for further information.

Mode Interface Configuration

Usage Use this command to send traffic to another device connected to the mirror port for monitoring.

See **"Port Mirroring" on page 14.17**.

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port, it is automatically removed from any VLAN it was associated with.

This command can only be applied to a single mirror (destination) port, not to a range of ports, nor to a static or dynamic channel group. Do not apply multiple interfaces with an interface command before issuing the mirror interface command. One interface may have multiple mirror interfaces.

Example To mirror traffic received and transmitted on `port1.0.4` and `port1.0.5` to destination `port1.0.3`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface port1.0.4,port1.0.5
                   direction both
```

To enable use with the **access-list (hardware IP numbered)** ACL and **default-action** QoS commands to destination `port1.0.3` without specifying a source port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface none
```

To mirror all TCP traffic, received or transmitted to analyzer `port1.0.1`, see the sample config below:

```
awplus#show running-config

!
mls qos enable
access-list 3000 copy-to-mirror tcp any any
access-group 3000
!
interface port1.0.1
 mirror interface none
 switchport
!
```

Related Commands

access-list (hardware IP numbered)
access-list (hardware MAC numbered)
default-action

platform stop-unreg-mc-flooding

This command stops multicast packets flooding out of all the ports in the VLAN until these packets are registered. This command does this by sending unregistered multicast packets to the switch processor, so there is no flooding of the multicast traffic onto the VLAN. Unregistered traffic will not flow until the switch has registered it, regardless of attempts to subscribe to it. Once the traffic is registered, it flows to registered subscribers and ports.

Use the **no** variant of this command to revert to default behavior and disable this feature.

Note

This command should not be used within any IPv6 networks.
IPv6 neighbor discovery operation is inhibited by this feature.
This command does not stop reserved Local Network Control Block IPv4 multicast packets in the address range 224.0.0.1 to 224.0.0.255 (224.0.0/24).
See **www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1**

Syntax

```
platform stop-unreg-mc-flooding

no platform stop-unreg-mc-flooding
```

Default This feature is disabled by default.

Mode Global Configuration

Usage This command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group. If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.

For further information about query messages see the **Staying in the Multicast Group (Query Message)** section in **Chapter 32, IGMP Snooping Introduction**.

This command also stops the initial flood of multicast packets that happens when a new multicast source starts to send traffic. This flooding lasts until snooping recognizes the multicast group. For example, in sites where IP cameras have multicast groups, traffic is flooded to the VLAN and causes large bursts of traffic. Use this command when there is limited processing available for large bursts of traffic, such as in sites with IP cameras.

Output See the console message warning about IPv6 operation after entering this command:

```
% WARNING: IPv6 will not work with this setting enabled
% Please consult the documentation for more information
```

See these sample console messages when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries:

```
awplus: [MLD-EVENTS] Grp - Rec Liveness Timer: Expiry for Grp ff0e::1 on port1.2.7
awplus: [IGMP-EVENTS] : Expiry (Unreg MC Timer) for Grp 224.2.2.2 on vlan4
```

Examples To enable this feature and stop multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# platform stop-unreg-mc-flooding
```

To disable this feature and allow multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# no platform stop-unreg-mc-flooding
```

Related Commands **show platform**
show running-config

polarity

This command sets the MDI/MDIX polarity on a copper-based switch port.

Syntax `polarity {auto|mdi|mdix}`

Parameter	Description
`mdi`	Sets the polarity to MDI (medium dependent interface).
`mdix`	Sets the polarity to MDI-X (medium dependent interface crossover).
`auto`	The switch port sets the polarity automatically. This is the default option.

Default By default, switch ports set the polarity automatically (**auto**).

Mode Interface Configuration

Usage We recommend the default **auto** setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; It does not apply to fiber ports. For more information, see **"MDI/MDIX Connection Modes" on page 14.5**.

Example To set the polarity for `port1.0.6` to fixed MDI mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# polarity mdi
```

show flowcontrol interface

Use this command to display flow control information.

Syntax `show flowcontrol interface <port>`

Parameter	Description
<port>	Specifies the name of the port to be displayed.

Mode User Exec and Privileged Exec

Example To display the flow control for the `port1.0.5`, use the command:

```
awplus# show flowcontrol interface port1.0.5
```

Output **Figure 15-1: Example output from the show flowcontrol interface command for a specific interface**

```
Port     Send  FlowControl    Receive  FlowControl  RxPause TxPause
          admin    oper        admin    oper
-----     ------- --------    ------- --------     ------- -------
port1.0.5 on       on           on       on           0       0
```

show loop-protection

Use this command to display the current loop protection setup for the device.

Syntax `show loop-protection [interface <port-list>] [counters]`

Parameter	Description
`interface`	The interface selected for display.
`<port-list>`	A port, a port range, or an aggregated link.
`counters`	Displays counter information for loop protection.

Mode User Exec and Privileged Exec

Usage This command is used to display the current configuration and operation of the Loop Protection feature

Examples To display the current configuration status for `port1.0.1`, use the command:

```
awplus# show loop-protection interface port1.0.1
```

Figure 15-2: Example output from the show loop-protection command

```
Loop-Detection:          Enabled
LDF Interval:            10 [sec]
Interface:               port1.0.1
 Action:                 port-disable
 Timeout:                300 [sec]
 Vlan:                   1
  Status:                Blocking
  Timeout Remaining:     115 [sec]
 Vlan:                   2
  Status:                Normal
  Timeout Remaining:     0 [sec]
```

To display the counter information for `port1.0.1`, use the command:

```
awplus# show loop-protection interface port1.0.1 counters
```

Figure 15-3: Example output from the show loop-protection interface counters command for port1.0.1

```
Interface:               port1.0.1
 Vlan:                   1
  LDF Tx:                3
  LDF Rx:                1
  Invalid LDF Rx:        1
  Action:                1
Vlan:                    2
  LDF Tx:                3
  LDF Rx:                0
  Invalid LDF Rx:        0
  Action:                0
```

show mac address-table

Use this command to display the mac address-table for all configured VLANs.

Syntax `show mac address-table`

Mode User Exec and Privileged Exec

Usage The **show mac address-table** command is only applicable to view a mac address-table for Layer 2 switched traffic within VLANs.

Example To display the mac address-table, use the following command:

```
awplus# show mac address-table
```

Output See the below sample output captured when there was no traffic being switched:

```
awplus#show mac address-table

VLAN Port          MAC               State
1    unknown       0000.cd28.0752    static
ARP  -             0000.cd00.0000    static
```

See the sample output captured when packets were switched and mac addresses were learned:

```
awplus#show mac address-table

VLAN Port          MAC              State
1    unknown       0000.cd28.0752   static
1    port1.0.6     0030.846e.9bf4   dynamic
1    port1.0.4     0030.846e.bac7   dynamic
ARP  -             0000.cd00.0000   static
```

Note the new mac addresses learned for `port1.0.4` and `port1.0.6` added as dynamic entries.

Note the first column of the output below shows VLAN IDs if multiple VLANs are configured:

```
awplus#show mac address-table

VLAN Port          MAC              State
1    unknown       0000.cd28.0752   static
1    port1.0.4     0030.846e.bac7   dynamic
2    unknown       0000.cd28.0752   static
2    port1.0.6     0030.846e.9bf4   dynamic
ARP  -             0000.cd00.0000   static
```

Also note manually configured static mac-addresses are shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int
port1.0.3 vlan 2
awplus(config)#end
awplus#
awplus#show mac address-table

VLAN Port          MAC              State
1    unknown       0000.cd28.0752   static
1    port1.0.2     0030.846e.bac7   dynamic
2    port1.0.3     0000.1111.2222   static
2    unknown       0000.cd28.0752   static
2    port1.0.5     0030.846e.9bf4   dynamic
ARP  -             0000.cd00.0000   statics
```

Related Commands

clear mac address-table dynamic
clear mac address-table static
mac address-table static

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 User Exec and Privileged Exec

Example To display the current, use the following command:

```
awplus# show mac address-table thrash-limit
```

Output **Figure 15-4: Example output from the show mac address-table thrash-limit command**

```
% Thrash-limit  7 movements per second
```

Related Commands mac address-table thrash-limit

show mirror

Use this command to display the status of all mirrored ports.

Syntax `show mirror`

Mode User Exec and Privileged Exec

Example To display the status of all mirrored ports, use the following command:

```
awplus# show mirror
```

Output **Figure 15-5: Example output from the show mirror command**

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.4
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.1
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.3
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: transmit
Monitored Port Name: port1.0.4
```

show mirror interface

Use this command to display port mirroring configuration for a mirrored (monitored) switch port.

Syntax `show mirror interface <port>`

Parameter	Description
<port>	The monitored switch port to display information about.

Mode User Exec, Privileged Exec and Interface Configuration

Example To display port mirroring configuration for the `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# show mirror interface port1.0.4
```

Output **Figure 15-6: Example output from the show mirror interface command**

```
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.4
```

show platform

This command displays the settings configured by using the **platform** commands.

Syntax `show platform`

Mode Privileged Exec

Usage This command displays the settings in the running config. For changes in some of these settings to take effect, the switch must be rebooted with the new settings in the startup config.

Example To check the settings configured with **platform** commands on the switch, use the following command:

```
awplus# show platform
```

show platform classifier statistics utilization brief

This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

Syntax `show platform classifier statistics utilization brief`

Mode Privileged Exec

Example To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

Output **Figure 15-7: Output from the show platform classifier statistics utilization brief command**

```
[Instance 3.0]
(Port1.0.1-1.0.24)
  Number of Entries:
  Policy Type      Group ID   Used / Total
  ---------------------------------------------
  ACL              1476395009    0 /  122 (  0%)
  DoS                      -1    0 /    0 (  0%)
  VLAN Counter             -1    0 /    0 (  0%)
  QoS                            0 /  768 (  0%)

[Instance 3.1]
(Port1.0.25-1.0.48)
  Number of Entries:
  Policy Type      Group ID   Used / Total
  ---------------------------------------------
  ACL              1476395009    0 /  122 (  0%)
  DoS                      -1    0 /    0 (  0%)
  VLAN Counter             -1    0 /    0 (  0%)
  QoS                            2 /  768 (  0%)
```

Related Commands show platform

show platform port

This command displays the various port registers or platform counters for specified switchports.

Syntax `show platform port [<port-list>|counters]`

Parameter	Description
<port-list>	The ports to display information about. A port-list can be: ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.6` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`.
`counters`	Show the platform counters.

Mode Privileged Exec

Examples To display port registers for `port1.0.1` and `port1.0.2` use the following command:

```
awplus# show platform port port1.0.1-port1.0.2
```

To display platform counters for `port1.0.1` and `port1.0.2` use the following command:

```
awplus# show platform port port1.0.1-port1.0.2 counters
```

Output **Figure 15-8: Example output from the show platform port command**

```
awplus#show platform port port1.0.1
Phy register value for port1.0.1 (ifindex: 5001)

00:1140  01:7949  02:0020  03:60B1  04:01E1  05:0000  06:0004  07:2001
08:0000  09:0600  10:0000  11:0000  12:0000  13:0000  14:0000  15:0000
16:0000  17:0000  18:0000  19:0000  20:0000  21:0000  22:0000  23:0000
24:0000  25:0000  26:0000  27:0000  28:0000  29:0000  30:0000  31:0000

Port configuration for lport 0x08001000:
  enabled:                1
  loopback:               0
  link:                   0
  speed:                  0  max speed:               1000
  duplex:                 0
  linkscan:               2
  autonegotiate:          1
  master:                 2
  tx pause:               1  rx pause:                   1
  untagged vlan:          1
  vlan filter:            3
  stp state:              1
  learn:                  5
  discard:                0
  max frame size:      1522
  MC Disable SA:         no
  MC Disable TTL:        no
  MC egress untag:        0
  MC egress vid:          0
  MC TTL threshold:      -1
```

Table 15-1: Parameters in the output from the show platform port command

Parameter	Description
Ethernet MAC counters	
`Combined receive/ transmit packets by size (octets) counters`	Number of packets in each size range received and transmitted.
`64`	Number of 64 octet packets received and transmitted.
`65 - 127`	Number of 65 - 127 octet packets received and transmitted.
`128 - 255`	Number of 128 - 255 octet packets received and transmitted.
`256 - 511`	Number of 256 - 511 octet packets received and transmitted.
`512 - 1023`	Number of 512 - 1023 octet packets received and transmitted.
`1024 - MaxPktSz`	Number of packets received and transmitted with size 1024 octets to the maximum packet length.
`1519 - 1522`	Number of 1519 - 1522 octet packets received and transmitted.
`1519 - 2047`	Number of 1519 - 2047 octet packets received and transmitted.
`2048 - 4095`	Number of 2048 - 4095 octet packets received and transmitted.
`4096 - 9216`	Number of 4096 - 9216 octet packets received and transmitted.
General Counters	
`Receive`	Counters for traffic received.
`Octets`	Number of octets received.
`Pkts`	Number of packets received.
`FCSErrors`	Number of FCS (Frame Check Sequence) error events received.
`UnicastPkts`	Number of unicast packets received.
`MulticastPkts`	Number of multicast packets received.
`BroadcastPkts`	Number of broadcast packets received.
`PauseMACCtlFrms`	Number of Pause MAC Control Frames received.
`OversizePkts`	Number of oversize packets received.
`Fragments`	Number of fragments received.
`Jabbers`	Number of jabber frames received.
`UnsupportOpcode`	Number of MAC Control frames with unsupported opcode received.
`AlignmentErrors`	Receive Alignment Error Frame Counter.
`SysErDurCarrier`	Receive Code Error Counter.

Table 15-1: Parameters in the output from the show platform port command (cont.)

Parameter	Description
CarrierSenseErr	Receive False Carrier Counter.
UndersizePkts	Number of undersized packets received.
Transmit	Counters for traffic transmitted.
Octets	Number of octets transmitted.
Pkts	Number of packets transmitted.
UnicastPkts	Number of unicast packets transmitted.
MulticastPkts	Number of multicast packets transmitted.
BroadcastPkts	Number of broadcast packets transmitted.
PauseMACCtlFrms	Number of Pause MAC Control Frames transmitted.
OversizePkts	Number of oversize packets transmitted.
FrameWDeferrdTx	Transmit Single Deferral Frame counter.
FrmWExcesDefer	Transmit Multiple Deferral Frame counter.
SingleCollsnFrm	Transmit Single Collision Frame counter.
MultCollsnFrm	Transmit Multiple Collision Frame counter.
LateCollisions	Transmit Late Collision Frame counter.
ExcessivCollsns	Transmit Excessive Collision Frame counter.
Collisions	Transmit Total Collision counter
Layer 3 Counters	
ifInUcastPkts	Inbound interface Unicast counter.
ifInDiscards	Inbound interface Discarded Packets counter.
ipInHdrErrors	Inbound interface Header Errors counter.
ifOutUcastPkts	Outbound interface Unicast counter.
ifOutErrors	Outbound interface Error counter.
Miscellaneous Counters	
DropEvents	Drop Event counter
ifOutDiscards	Outbound interface Discarded Packets counter.
MTUExcdDiscard	Receive MTU Check Error Frame Counter

Output **Figure 15-9: Example output from the show platform port counters command**

```
awplus#show platform port port1.0.1 counters

 Switch Port Counters
------------------------------------------------------------------------

Port port1.0.1 Ethernet MAC counters:
 Combined receive/transmit packets by size (octets) counters:
  64                              0 1024 - MaxPktSz                 0
  65 - 127                        0 1519 - 1522                     0
  128 - 255                       0 1519 - 2047                     0
  256 - 511                       0 2048 - 4095                     0
  512 - 1023                      0 4096 - 9216                     0

 General Counters:
 Receive                            Transmit
  Octets                          0 Octets                          0
  Pkts                            0 Pkts                            0
  FCSErrors                       0
  UnicastPkts                     0 UnicastPkts                     0
  MulticastPkts                   0 MulticastPkts                   0
  BroadcastPkts                   0 BroadcastPkts                   0
  PauseMACCtlFrms                 0 PauseMACCtlFrms                 0
  OversizePkts                    0
  Fragments                       0
  Jabbers                         0
  UnsupportOpcode                 0
  AlignmentErrors                 0
  SymErDurCarrier                 0
  CarrierSenseErr                 0
  UndersizePkts                   0
                                     FrameWDeferrdTx                0
                                     FrmWExcesDefer                 0
                                     SingleCollsnFrm                0
                                     MultCollsnFrm                  0
                                     LateCollisions                 0
                                     ExcessivCollsns                0
                                     Collisions                     0

 Layer 3 Counters:
  ifInUcastPkts                   0 ifOutUcastPkts                  0
  ifInDiscards                    0 ifOutErrors                     0
  ipInHdrErrors                   0

 Miscellaneous Counters:
  DropEvents                      0
  ifOutDiscards                   0
  MTUExcdDiscard                  0

------------------------------------------------------------------------
```

Table 15-2: Output parameters from the show platform port counters command

Parameter	Description
Ethernet MAC counters	
`Combined receive/transmit packets by size (octets) counters`	Number of packets in each size range received and transmitted.
`64`	Number of 64 octet packets received and transmitted.
`65 - 127`	Number of 65 - 127 octet packets received and transmitted.

Table 15-2: Output parameters from the show platform port counters command

Parameter	Description
128 - 255	Number of 128 - 255 octet packets received and transmitted.
256 - 511	Number of 256 - 511 octet packets received and transmitted.
512 - 1023	Number of 512 - 1023 octet packets received and transmitted.
1024 - MaxPktSz	Number of packets received and transmitted with size 1024 octets to the maximum packet length.
General Counters	
Receive	Counters for traffic received.
Octets	Number of octets received.
Pkts	Number of packets received.
CRCErrors	Number of CRC (Cyclic Redundancy Check) error events received.
UnicastPkts	Number of unicast packets received.
MulticastPkts	Number of multicast packets received.
BroadcastPkts	Number of broadcast packets received.
FlowCtrlFrms	Number of good Flow Control frames received.
OversizePkts	Number of oversize packets received.
Fragments	Number of fragments received.
Jabbers	Number of jabber frames received.
UnsupportOpcode	Number of MAC Control frames with unsupported opcode received.
UndersizePkts	Number of undersized packets received.
Transmit	Counters for traffic transmitted.
Octets	Number of octets transmitted.
Pkts	Number of packets transmitted.
UnicastPkts	Number of unicast packets transmitted.
MulticastPkts	Number of multicast packets transmitted.
BroadcastPkts	Number of broadcast packets transmitted.
FlowCtrlFrms	Number of good Flow Control frames transmitted.
OversizePkts	Number of oversize packets transmitted.
FlowCtrlFrms	The number of Flow Control frames transmitted.
Collisions	Total number of collisions seen by the MAC.
LateCollisions	Total number of late collisions seen by the MAC.
ExcessivCollsns	Number of frames dropped in the transmit MAC due to excessive collisions. This is applicable for Half-Duplex mode only.

Table 15-2: Output parameters from the show platform port counters command

Parameter	Description
Miscellaneous Counters	
`Mac TxErr`	Number of frames not transmitted correctly or dropped due to internal MAC transmit error.
`Mac RxErr`	Number of Receive Error events seen by the receive side of the MAC.
`DropEvents`	Number of instances that the port was unable to receive packets due to insufficient bandwidth to one of the PP internal resources, such as the DRAM or buffer allocation.

show port-security interface

Use this command to show the current port-security configuration and the switch port status.

Syntax `show port-security interface <port>`

Parameter	Description
`<port>`	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).

Mode Privileged Exec

Example To see the port-security status on `port1.0.1`, use the following command:

```
awplus# show port-security interface port1.0.1
```

Output **Figure 15-10: Example output from the show port-security interface command**

```
Port Security configuration
Security Enabled              : YES
Port Status                   : ENABLED
Violation Mode                : TRAP
Aging                         : OFF
Maximum MAC Addresses         : 3
Total MAC ddresses            : 1
Lock Status                   : UNLOCKED
Security Violation Count      : 0
Last Violation Source Address : None
```

show port-security intrusion

Shows the intrusion list. If the port is not specified, the entire intrusion table is shown.

Syntax `show port-security intrusion [interface <port>]`

Parameter	Description
`interface`	Specify a port
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).

Mode Privileged Exec

Example To see the intrusion list on `port1.0.1`, use the following command:

```
awplus# show port-security intrusion interface port1.0.1
```

Output **Figure 15-11: Example output from the show port-security intrusion command for port 1.0.1**

```
Port Security Intrusion List
Interface: port1.0.1 -3 intrusion(s) detected
11-22-33-44-55-04 11-22-33-44-55-06 11-22-33-44-55-08
```

show storm-control

Use this command to display storm-control information for all interfaces or a particular interface.

Syntax `show storm-control [<port>]`

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec and Privileged Exec

Example To display storm-control information for `port1.0.2`, use the following command:

```
awplus# show storm-control port1.0.2
```

Output **Figure 15-12: Example output from the show storm-control command for port1.0.2**

```
Port       BcastLevel  McastLevel  DlfLevel
port1.0.2      40. 0%     100. 0%   100. 0%
```

Example To display storm-control information for all ports, use the following command:

```
awplus# show storm-control
```

Output **Figure 15-13: Example output from the show storm-control command for all ports**

```
awplus#show storm-control
Port       BcastLevel  McastLevel  DlfLevel
port1.0.1      100.0%      100.0%    100.0%
port1.0.2      100.0%      100.0%    100.0%
port1.0.3      100.0%      100.0%    100.0%
port1.0.4      100.0%      100.0%    100.0%
port1.0.5      100.0%      100.0%    100.0%
port1.0.6      100.0%      100.0%    100.0%
port1.0.7      100.0%      100.0%    100.0%
port1.0.8      100.0%      100.0%    100.0%
port1.0.9      100.0%      100.0%    100.0%
port1.0.10     100.0%      100.0%    100.0%
port1.0.11     100.0%      100.0%    100.0%
port1.0.12     100.0%      100.0%    100.0%
port1.0.13     100.0%      100.0%    100.0%
port1.0.14     100.0%      100.0%    100.0%
port1.0.15     100.0%      100.0%    100.0%
port1.0.16     100.0%      100.0%    100.0%
port1.0.17     100.0%      100.0%    100.0%
port1.0.18     100.0%      100.0%    100.0%
port1.0.19     100.0%      100.0%    100.0%
port1.0.20     100.0%      100.0%    100.0%
port1.0.21     100.0%      100.0%    100.0%
port1.0.22     100.0%      100.0%    100.0%
port1.0.23     100.0%      100.0%    100.0%
port1.0.24     100.0%      100.0%    100.0%
```

Related Commands **storm-control level**

speed

This command changes the speed of the specified port. You can optionally specify the speed or speeds that get autonegotiated, so autonegotiation is only attempted at the specified speeds.

To see the currently-negotiated speed for ports whose links are up, use the **show interface** command. To see the configured speed (when different from the default), use the **show running-config** command.

Syntax `speed {10|100|1000|10000|auto [10][100][1000][10000]}`

The following table shows the speed options for each type of port.

Port type	Speed Options (units are Mbps)
RJ-45 and RJ.5copper ports	auto (default) 10 100 1000
supported tri-speed copper SFPs	auto (default) 10 100 1000
100Mb fiber SFPs	100
1000Mb fiber SFPs	auto (default) 1000
10000Mb fiber SFP+	auto (default) 10000

Mode Interface Configuration

Default By default, ports autonegotiate speed (except for 100Base-FX ports which do not support auto-negotiation, so default to 100Mbps).

Usage Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the speed of all the switch ports in the channel group by applying this command to the channel group.

Note Note that if multiple speeds are specified after the auto option to autonegotiate speeds, then only those speeds specified are attempted for autonegotiation.

Examples To set the speed of a tri-speed port to 100Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed 100
```

To return the port to auto-negotiating its speed, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto
```

To set a port to auto-negotiate its speed at 100Mbps and 1000Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 100 1000
```

To set a port to auto-negotiate its speed at 1000Mbps only, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 1000
```

Related Commands

duplex
ecofriendly lpi
polarity
show interface
speed (asyn)

storm-control level

Use this command to specify the threshold level for broadcasting, multicast, or destination lookup failure (DLF) traffic for the port. Storm-control limits the specified traffic type to the specified threshold.

Use the **no** variant of this command to disable storm-control for broadcast, multicast or DLF traffic.

Syntax

```
storm-control {broadcast|multicast|dlf} level <level>
no storm-control {broadcast|multicast|dlf} level
```

Parameter	Description
<level>	<0-100> Specifies the threshold as a percentage of the maximum port speed.
broadcast	Applies the storm-control to broadcast frames.
multicast	Applies the storm-control to multicast frames.
dlf	Applies the storm-control to destination lookup failure traffic.

Default By default, storm-control is disabled.

Mode Interface Configuration

Usage Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Example To limit broadcast traffic on `port1.0.2` to 30% of the maximum port speed, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# storm-control broadcast level 30
```

Related Commands show storm-control

thrash-limiting

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
`action`	The mac thrashing detected action. The default is vlan-disable.
`learn-disable`	Disable mac address learning
`link-down`	Block all traffic on an interface - link down
`port-disable`	Block all traffic on an interface - link remains up
`vlan-disable`	Block all traffic on a vlan. Note that setting this parameter will also enable ingress filtering.
`none`	No thrash action
`timeout`	Set the duration for the thrash action
<0-86400>	The duration of the applied thrash action in seconds. The default is 1 seconds.

Default The default action is learn-disable.

Mode Interface Configuration

Usage See the **Thrash Limiting** section in **Chapter 14, Switching Introduction** for relevant conceptual, configuration, and overview information prior to applying this command.

Examples To set the action to learn disable for `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# thrash-limiting action learn-disable
```

To block all traffic on a vlan, use the following command:

```
awplus# configure terminal
awplus(config)# thrash-limiting action vlan-disable
```

To set the thrash limiting timeout to 5 seconds, use the following command:

```
awplus(config-if)# thrash-limiting timeout 5
```

To set the thrash limiting action to its default, use the following command:

```
awplus(config-if)# no thrash-limiting action
```

To set the thrash limiting timeout to its default, use the following command:

```
awplus(config-if)# no thrash-limiting timeout
```

Related Commands

loop-protection
loop-protection action
loop-protection timeout
show loop-protection

Chapter 16: VLAN Introduction

VLANs Introduction 16.2
Virtual LANs (VLANs) 16.2
Configuring VLANs 16.3
Private VLANs 16.5
Private VLANs for Ports in Access Mode 16.5
Private VLAN Operation with Ports in Access Mode 16.7
Access Mode Private VLAN Configuration Example 16.8
Private VLANs for Trunked Ports 16.11
Trunked Port Private VLAN Configuration Example 16.12
Protocol Based VLAN Configuration Example 16.16

VLANs Introduction

This chapter describes Virtual LANs (VLAN), VLAN features and configuration on the switch. For detailed descriptions of commands used to configure VLANs, see **Chapter 17, VLAN Commands**. For information about Voice VLAN and LLDP-MED, see **Chapter 69, LLDP, LLDP-MED and Voice VLAN Introduction and Configuration**.

Virtual LANs (VLANs)

A Virtual LAN (VLAN) is a logical, software-defined subnetwork. It allows similar devices on the network to be grouped together into one broadcast domain, irrespective of their physical position in the network. Multiple VLANs can be used to group workstations, servers, and other network equipment connected to the switch, according to similar data and security requirements.

Decoupling logical broadcast domains from the physical wiring topology offers several advantages, including the ability to:

- Move devices and people with minimal, or no, reconfiguration
- Change a device's broadcast domain and access to resources without physically moving the device, by software reconfiguration or by moving its cable from one switch port to another
- Isolate parts of the network from other parts, by placing them in different VLANs
- Share servers and other network resources without losing data isolation or security
- Direct broadcast traffic to only those devices which need to receive it, to reduce traffic across the network
- Connect 802.1Q-compatible switches together through one port on each switch

Devices that are members of the same VLAN only exchange data with each other through the switch's Layer 2 switching capabilities. To exchange data between devices that are located in different VLANs, the switch's Layer 3 (routing) capabilities are used.

Different IP subnets are associated with different VLANs. The switch's IP router table will be populated by the routes to the subnets on any active VLANs, and by routes statically configured over active VLAN interfaces, or learned via routing protocols operating over these interfaces.

The device supports up to 4094 VLANs (the maximum allowed by the VID field in the 802.1Q tag). On some devices a few of these VLANs may be reserved for management purposes.

When the switch is first powered up (and therefore unconfigured), it creates a default VLAN with a VID of 1 and an interface name of *vlan1*. In this initial condition, the switch attaches all its ports to this default VLAN.

The default VLAN cannot be deleted, and ports can only be removed from it if they also belong to at least one other VLAN. If all the devices on the physical LAN belong to the same logical LAN, that is, the same broadcast domain, then the default settings will be acceptable, and no additional VLAN configuration is required.

Configuring VLANs

Defaults

By default, all switch ports are in access mode, are associated with the default VLAN (**vlan1**), and have ingress filtering on. You cannot delete **vlan1**.

VLAN names

When you create a VLAN (using the **vlan** command), you give it a numerical VLAN Identifier (VID) - a number from 2 to 4094. If tagged frames are transmitted from this VLAN, they will contain this VID in their tag. You may also give it an arbitrary alphanumeric name containing a meaningful description, which is not transmitted to other devices.

When referring to a VLAN, some commands require the VLAN to be specified by its VID while some commands require it to be specified by its interface name: vlan<VID>. In command output, the VLAN may be referred to by its VID, its interface name (vlan<VID>), or its VLAN name (the arbitrary alphanumeric string).

You can name a VLAN with a string containing “vlan” and its VLAN Identifier (VID). To avoid confusion, we recommend not naming it “vlan” followed by any number different from its VID.

Access mode

A switch port in access mode sends untagged Ethernet frames, that is, frames without a VLAN tag. Each port is associated with one VLAN (the port-based VLAN, by default, *vlan1*), and when it receives untagged frames, it associates them with the VID of this VLAN. You can associate the port with another VLAN (using the **switchport access vlan** command). This removes it from the default VLAN.

Use access mode for any ports connected to devices that do not use VLAN tagging, for instance PC workstations.

Trunk mode

A switch port in trunk mode is associated with one or more VLANs for which it transmits VLAN-tagged frames, and for which it identifies incoming tagged frames with these VIDs.

To allow a switch port to distinguish and identify traffic from different VLANs, put it in trunk mode (using the **switchport mode trunk** command), and add the VLANs (using the **switchport trunk allowed vlan** command). Use trunk mode for ports connected to other switches which send VLAN-tagged traffic from one or more VLANs.

A trunk mode port may also have a native VLAN (by default vlan1), for which it transmits untagged frames, and with which it associates incoming untagged frames (using the **switchport trunk native vlan** command).

Ports in trunk mode can be enabled as promiscuous ports for private VLANs (using the **switchport mode private-vlan trunk promiscuous**) and secondary ports for private VLANs (using the **switchport mode private-vlan trunk secondary**).

Mirror ports

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port (using the **mirror interface** command), it is automatically removed from any VLAN it was associated with.

VLANs and channel groups

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Table 16-1: Configuration procedure for VLANs

Step 1. Create VLANs	
`awplus#` **`configure terminal`**	Enter Configuration mode.
`awplus(config)#` `vlan database`	Enter VLAN Configuration mode.

`awplus(config-vlan)#`
`vlan <vid> [name <vlan-name>] [state {enable|disable}]`
or
`vlan <vid-range> [state {enable|disable}]`
	Create VLANs.

Step 2. Associate switch ports with VLANs	
`awplus(config-vlan)#` `interface <port-list>`	Associate switch ports in access mode with VLANs:
`awplus(config-if)#` `switchport access vlan <vlan-id>`	Enter Interface Configuration mode for the switch ports that will be in access mode for a particular VLAN. Associate the VLAN with these ports in access mode. Repeat for other VLANs and ports in access mode.
`awplus(config-if)#` `interface <port-list>`	Associate switch ports in trunk mode with VLANs. Enter Interface Configuration mode for all the switch ports that will be in trunk mode for a particular set of VLANs.
`awplus(config-if)#` `switchport mode trunk [ingress-filter {enable|disable}]`	Set these switch ports to trunk mode.

`awplus(config-if)#`
`switchport trunk allowed vlan all`
or
`switchport trunk allowed vlan add <vid-list>`
	Allow these switch ports to trunk this set of VLANs.

`awplus(config-if)#` `switchport trunk native vlan {<vid>|none}`	By default, a trunk mode switch port's native VLAN, the VLAN that the port uses for untagged packet, is VLAN 1. If required, change the native VLAN from the default.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show vlan {all|brief|dynamic|static|auto|static-ports<1-4094>}`	Confirm VLAN configuration.

Private VLANs

Private VLANs combine the network advantages of conventional VLANs, with an added degree of privacy obtained by limiting the connectivity between selected ports.

This section provides an introduction to:

- Private VLANs for ports in access mode
- **Private VLANs for Trunked Ports**

Private VLANs for Ports in Access Mode

An example application of a private VLAN would be a library in which user booths each have a PC with Internet access. In this situation it would usually be undesirable to allow communication between these individual PCs. Connecting the PC to ports within a private isolated VLAN would enable each PC to access the Internet or a library server via a single connection, whilst preventing access between the PCs in the booths.

Another application might be to use private VLANs to simplify IP address assignment. Ports can be isolated from each other whilst still belonging to the same subnet.

A private VLAN comprises the following components:

- **a single promiscuous port**
- **one or more host ports.** There are two types of host port:
  - **isolated ports**: These can only communicate with the promiscuous port that is associated with the isolated VLAN.
  - **community ports:** These can communicate with their associated promiscuous port and other community ports within the community VLAN.
- **a single primary VLAN**
- **one or more secondary VLANs:** There are two types of secondary VLAN:
  - **isolated VLANs:** In this VLAN type, communication can only take place between each host port and its associated promiscuous port.
  - **community VLANs:** In this VLAN type, communication can take place between host ports and between each host port and its associated promiscuous port.

Membership rules for private VLANs in access mode

The following membership rules apply when creating and operating private VLANs in access mode.

Each private VLAN:

- must contain one promiscuous port (or aggregated link)
- may contain multiple host ports
- can be configured to span switch instances
- can only contain promiscuous and host ports
- cannot use the default VLAN (vlan1)
- a private *isolated* VLAN can only contain a single promiscuous port
- a private *community* VLAN can contain more than one promiscuous port

A promiscuous port:

- is a member of the primary VLAN and all its associated secondary VLANs
- cannot be a member of both private and non-private VLANs

A host port:

- can be a member of multiple private (community) VLANs, but all these VLANs must share the same promiscuous port
- cannot be a host port in some VLANs and a non-host port in others
- cannot be a promiscuous port in another VLAN

Promiscuous ports

A promiscuous port can communicate with all ports that are members of its associated secondary VLANs. Multiple promiscuous ports can exist in a primary VLAN, but only if the primary VLAN is only associated with community VLANS (that is, that there are no isolated VLANs associated with this port).

A promiscuous port is a member of the primary VLAN and all associated secondary VLANs. Its Port VID is set to the VLAN ID of the primary VLAN.

Host ports

Host ports have two levels of connectivity depending on whether they exist in an isolated or a community VLAN.

1. Host ports within an isolated VLAN

These ports are only allowed to communicate with their VLAN's promiscuous port, even though they share their secondary (isolated) VLAN with other hosts. The host ports receive their data from the promiscuous port via the primary VLAN, and individually transmit their data to the promiscuous port via their common secondary VLAN.

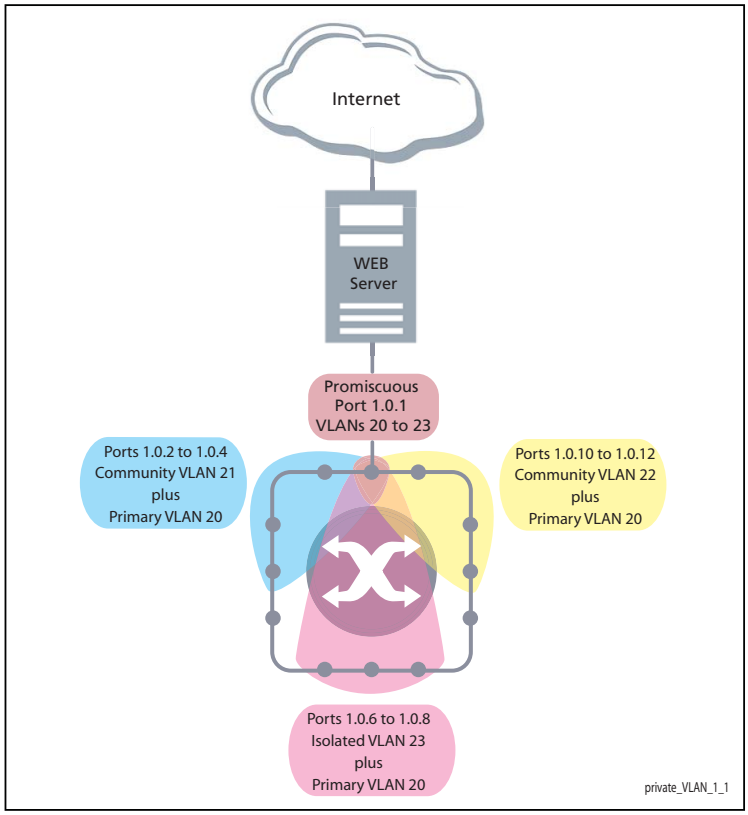
2. Host ports within a community VLAN

These ports are able to communicate with both the promiscuous port and the other ports within the community VLAN that they are associated with. They receive their data from the promiscuous port via the primary VLAN, and transmit their data to both the promiscuous port and the other host ports (within their community VLAN) via their common secondary VLAN. However, the only external path from a community VLAN is from its promiscuous port.

Private VLAN Operation with Ports in Access Mode

A basic private VLAN operation is shown in the following figure. It comprises a primary VLAN 20 plus community and isolated VLANS.

Figure 16-1: Private VLAN



The ports on this switch have the following configuration:

- Port 1.0.1 is the promiscuous port and is a member of the primary VLAN 20 and all its associated secondary VLANs.
- Ports 1.0.2 to 1.0.4 are members of the community VLAN 21 and are able to communicate with both the promiscuous port and all other ports in VLAN 21.
- Ports 1.0.10 to 1.0.12 are members of the community VLAN 22 and are able to communicate with both the promiscuous port and all other ports in VLAN 22.
- Ports 1.0.6 to 1.0.8 are members of the isolated VLAN 23. Each of these ports can only communicate with the promiscuous port.

Table 16-2: Private VLANs - Port Tagging

Port	Mode	Untagged VLAN Membership	PVID
1.0.1	Promiscuous	20, 21, 22, 23	20
1.0.2 to 1.0.4	Host	20, 21	21
1.0.10 to 1.0.12	Host	20, 22	22
1.0.6 to 1.0.8	Host	20, 23	23
1.0.5	Not members of the private VLAN		-
1.0.9	Not members of the private VLAN		-

Private VLANs operate within a single switch and comprise one primary VLAN plus a number of secondary VLANS. All data enters the private VLAN ports untagged.

Using the example of **Figure 16-1**, data enters the switch via the promiscuous `port1.0.1` and is forwarded to the host ports using VLAN 20, the primary VLAN. Data returning from the host ports to the promiscuous port (and exiting the switch) use the secondary VLAN associated with its particular host port, VLAN 21, 22, or 23 in the example.

Thus the data flows into the switch via the primary VLAN and out of the switch via the secondary VLANs. This situation is not detected outside of the switch, because all its private ports are untagged. Note however, that data flowing between ports within the same community VLAN will do so using the VID of the community VLAN.

Portfast on private VLANS

Within private VLANs, we recommend that you place all host ports into spanning-tree portfast mode and enable BPDU guard. Portfast assumes that because host ports will also be edge ports, they will have no alternative paths (loops) via other bridges. These ports are therefore allowed to move directly from the spanning-tree blocking state into the forwarding state, thus bypassing the intermediate states.

Applying BPDU guard is an extra precaution. This feature disables an edge port if it receives a BPDU frame, because receiving such a frame would indicate that the port has a connection to another network bridge.

For more information on BPDU guard and portfast, see their following commands:

- **spanning-tree portfast bpdu-guard** command on page 19.64
- **spanning-tree portfast (STP)** command on page 19.60

Access Mode Private VLAN Configuration Example

Table 16-3: Configuration procedure for access mode private VLANs

Command	Description
Step 1. Create the VLANs	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `vlan database`	Enter VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 20-23`	Create the VLANs.
Step 2. Create the private VLANs and set the type	
`awplus(config-vlan)#` `private-vlan 20 primary`	Create primary VLAN 20.
`awplus(config-vlan)#` `private-vlan 21 community`	Create community VLAN 21.
`awplus(config-vlan)#` `private-vlan 22 community`	Create community VLAN 22.

Table 16-3: Configuration procedure for access mode private VLANs (cont.)

Command	Description
`awplus(config-vlan)#` `private-vlan 23 isolated`	Create isolated VLAN 23.
Step 3. Associate the secondary VLANs with the primary VLAN	
`awplus(config-vlan)#` `private-vlan 20 association add 21`	Associate secondary VLAN 21 with the primary VLAN 20.
`awplus(config-vlan)#` `private-vlan 20 association add 22`	Associate secondary VLAN 22 with the primary VLAN 20.
`awplus(config-vlan)#` `private-vlan 20 association add 23`	Associate secondary VLAN 23 with the primary VLAN 20.
Step 4. Set port 1.0.1 to be the promiscuous port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.1`	Enter Interface Configuration mode for `port1.0.1`.
`awplus(config-if)#` `switchport mode private-vlan promiscuous`	Set the port as a promiscuous ports.
Step 5. Set the other ports to be host ports	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.2-1.0.4, port1.0.6`	Enter Interface Configuration mode for the ports.
`awplus(config-if)#` `switchport mode private-vlan host`	Set the ports as host ports.
Step 6. On the promiscuous port, map the primary VLAN to each of the secondary VLANs	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.1`	Enter Interface Configuration mode for `port1.0.1`.

Table 16-3: Configuration procedure for access mode private VLANs (cont.)

Command	Description
`awplus(config-if)#` `switchport private-vlan mapping 20 add 21-23`	Associate primary VLAN 20 and the secondary VLANs 21 to 23 to the promiscuous port.
Step 7. Associate the community host ports with the community VLANs	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.2-1.0.4`	Enter Interface Configuration mode for ports 1.0.2 to 1.0.4.
`awplus(config-if)#` `switchport private-vlan host-association 20 add 21`	Associate primary VLAN 20 and secondary VLAN 21 to the host ports.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.10-1.0.12`	Enter Interface Configuration mode for ports 1.0.10 to 1.0.12.
`awplus(config-if)#` `switchport private-vlan host-association 20 add 22`	Associate primary VLAN 20 and secondary VLAN 22 to the host ports.
Step 8. Associate the isolated host ports with the isolated VLAN 23	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.6-1.0.8`	Enter Interface Configuration mode for ports 1.0.6 to 1.0.8.
`awplus(config-if)#` `switchport private-vlan host-association 20 add 23`	Associate primary VLAN 20 and secondary VLAN 23 to the host ports.

Private VLANs for Trunked Ports

Private VLAN trunk ports allow you to combine traffic for private isolated VLANs over a trunk. A port in trunk mode enabled as a promiscuous port with the **switchport mode private-vlan trunk promiscuous** command can carry both multiple isolated private VLANs and non-private VLANs. A promiscuous port in trunk mode allows you to combine multiple isolated VLANs on a single trunk port. A port in trunk mode enabled as a secondary port with the **switchport mode private-vlan trunk secondary** command can combine traffic for multiple isolated VLANs over a trunk.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

A private VLAN group for trunked ports comprises the following components:

- **a single promiscuous port**
- **one or more isolated secondary ports:** These can only communicate with the associated promiscuous port.
- **isolated VLANs:** In this VLAN type, communication can only take place between each secondary port and its associated promiscuous port. Membership rules for private VLANs for trunked ports

The following membership rules apply when creating and operating private VLANs for trunked ports.

A promiscuous trunk port:

- must be in trunk mode
- can be a member of both isolated VLANs and non-isolated VLANs
- has a group ID that is solely used to associate the promiscuous port with secondary ports

A secondary trunk port:

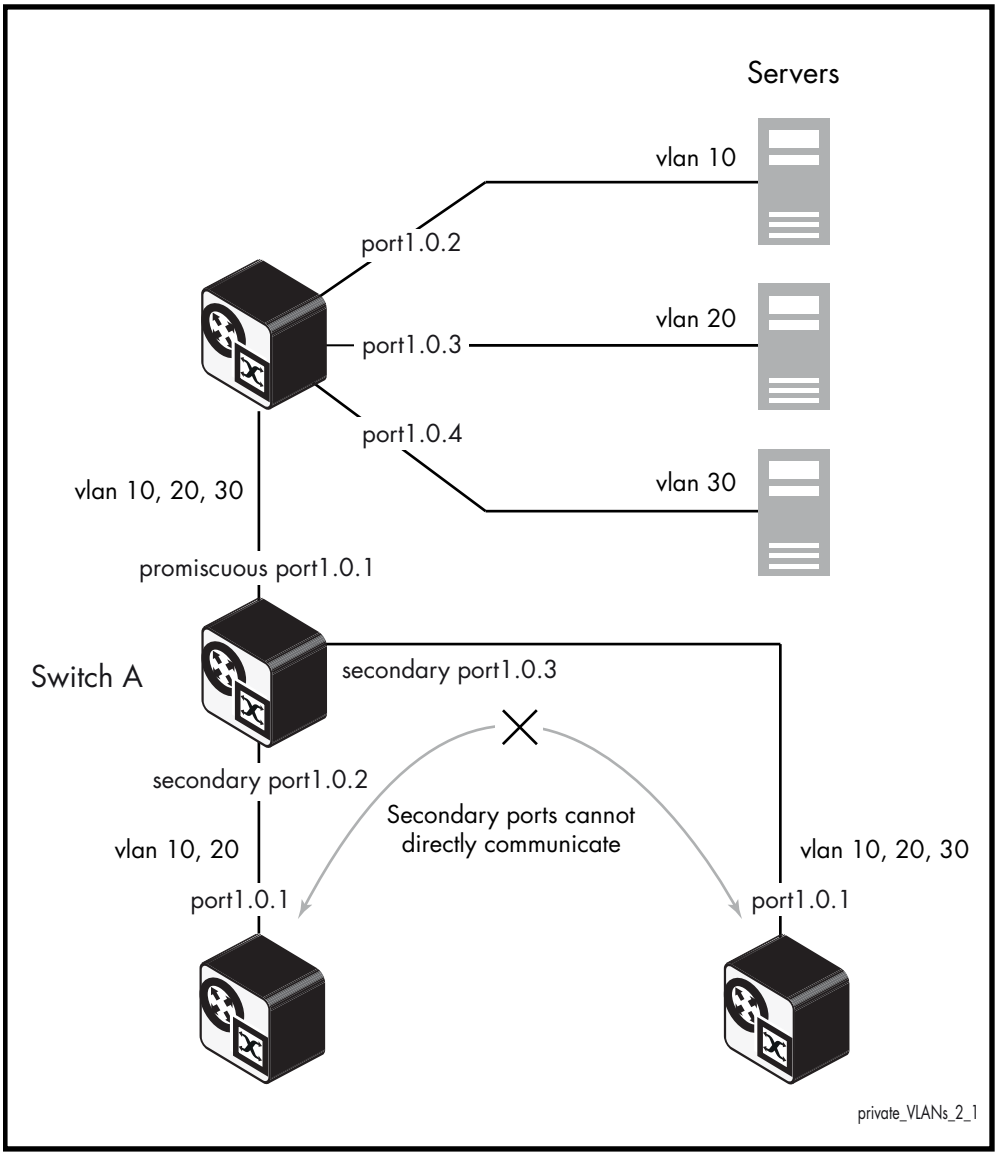
- must be in trunk mode
- can only be a member of isolated VLANs
- cannot be a promiscuous port in another VLAN
- has a group ID that is solely used to associate the secondary port with its promiscuous port

Unlike private VLANs for ports in access mode, private VLANs for trunked ports have no secondary to primary VLAN mappings.

Trunked Port Private VLAN Configuration Example

A basic trunked port private VLAN operation is shown in the following figure.

Figure 16-2: Trunked port private VLAN



The ports on **Switch A** have the following configuration:

- Port 1.0.1 is the promiscuous port, and has a group ID of 1
- Port 1.0.2 is a secondary port for isolated private VLANs 10 and 20, and has a group ID of 1
- Port 1.0.3 is a secondary port for isolated private VLANs 10, 20 and 30, and has a group ID of 1

The configuration procedure in **Table 16-4** show the steps to configure **Switch A**.

Table 16-4: Configuration procedure for Switch A

Command	Description
Step 1. Create the VLANs	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `vlan database`	Enter VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 10,20,30`	Create the VLANs.
Step 2. Create the private VLANs and set the type	
`awplus(config-vlan)#` `private-vlan 10 isolated`	Create isolated VLAN 10.
`awplus(config-vlan)#` `private-vlan 20 isolated`	Create isolated VLAN 20.
`awplus(config-vlan)#` `private-vlan 30 isolated`	Create isolated VLAN 30.
`awplus(config-vlan)#` `interface port1.0.1`	Enter Interface Configuration mode for `port1.0.1`.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of the port to trunk.
`awplus(config-if)#` `switchport trunk allowed vlan add 10,20,30`	Add the VLANs to be trunked over this port.
Step 3. Set port 1.0.2 to trunk mode and add the VLANs to be trunked over the port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.2`	Enter Interface Configuration mode for `port1.0.2`.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of the port to trunk.
`awplus(config-if)#` `switchport trunk allowed vlan add 10,20`	Add the VLANs to be trunked over this port.

Table 16-4: Configuration procedure for Switch A(cont.)

Command	Description
Step 4. Set port 1.0.3 to trunk mode and add the VLANs to be trunked over the port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.3`	Enter Interface Configuration mode for port 1.0.3.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of the port to trunk.
`awplus(config-if)#` `switchport trunk allowed vlan add 10,20,30`	Add the VLANs to be trunked over this port.
Step 5. Set port 1.0.1 to be the promiscuous port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.1`	Enter Interface Configuration mode for port 1.0.1.
`awplus(config-if)#` `switchport mode private-vlan trunk promiscuous group 1`	Enable the port in trunk mode to be promiscuous port for isolated VLANs 10, 20 and 30 with a group ID of 1.
Step 6. Set port 1.0.2 to be a secondary port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface port1.0.2`	Enter Interface Configuration mode for `port1.0.2`.
`awplus(config-if)#` `switchport mode private-vlan trunk secondary group 1`	Enable the port in trunk mode to be a secondary port for isolated VLANs 10 and 20 with a group ID of 1.
Step 7. Set port 1.0.3 to be a secondary port	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.

Table 16-4: Configuration procedure for Switch A(cont.)

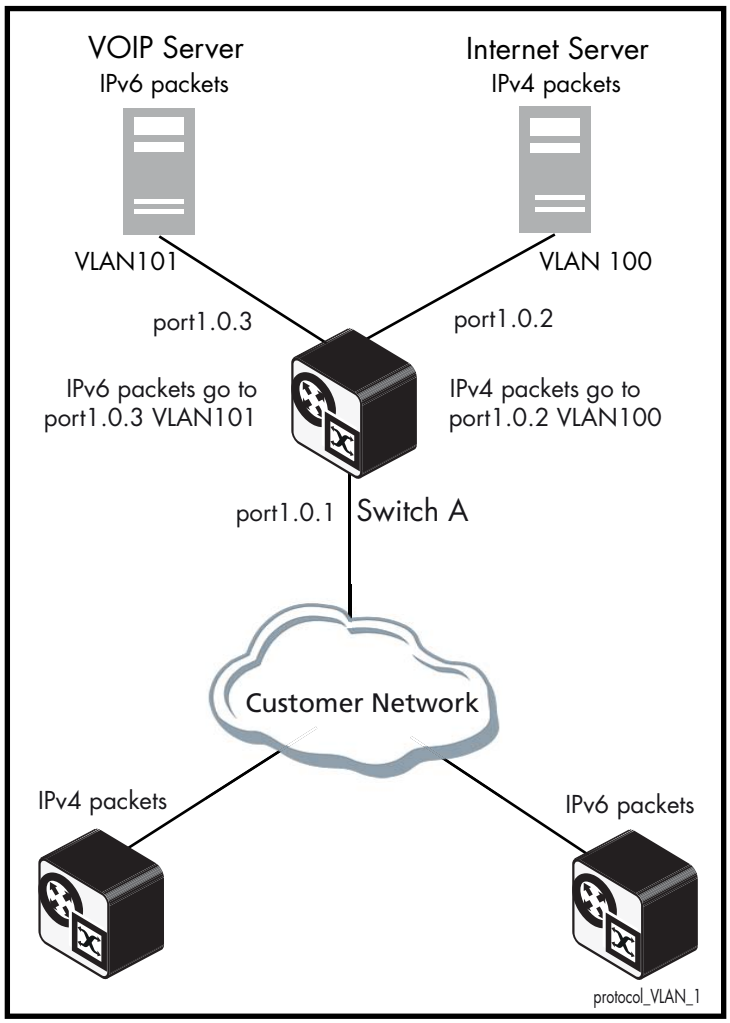
Command	Description
`awplus(config)#` `interface port1.0.3`	Enter Interface Configuration mode for `port1.0.3`.
`awplus(config-if)#` `switchport mode private-vlan trunk secondary group 1`	Enable the port in trunk mode to be a secondary port for isolated VLANs 10, 20 and 30 with a group ID of 1.

Protocol Based VLAN Configuration Example

A protocol based VLAN topology is shown below in **Figure 16-3**.

See the configuration procedure to configure **Switch A** in **Table 16-4**

Figure 16-3: Protocol based VLAN configuration



Switch A has the following configuration to enable protocol based VLAN classification:

- VLAN 100 and VLAN 101 created and applied to port1.0.2 and port1.0.3 respectively
- IPv4 and IPv6 VLAN classifier rules created and mapped to VLAN 100 and VLAN 101
- VLAN classifier group created and mapped to port1.0.1
- VLAN 100 and VLAN 101 are trunked over port1.0.2 and port1.0.3 respectively
- IPv4 packets received on port1.0.1 go to port1.0.2 VLAN 100
- IPv6 packets received on port1.0.1 go to port1.0.3 VLAN 101

The configuration procedure in **Table 16-4** show the steps to configure **Switch A**.

Table 16-5: Configuration procedure for Switch A

Command	Description
Step 1. Create the VLANs 100 and 101	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `vlan database`	Enter VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 100,101`	Create the VLANs.
`awplus(config-vlan)#` `exit`	Exit VLAN Configuration mode.
Step 2. Create two protocol type based VLAN classifier rules for IPv4 and IPv6 mapped to VLAN 100 and 101	
`awplus(config)#` `vlan classifier rule 1 proto ip encap ethv2 vlan 100`	Create a VLAN classifier rule `1` for IPv4 packets on VLAN `100`.
`awplus(config)#` `vlan classifier rule 2 proto ipv6 encap ethv2 vlan 101`	Create a VLAN classifier rule `2` for IPv6 packets on VLAN `101`.
Step 3. Create a group of VLAN classifier rules and map the defined VLAN classifier rules 1 and 2 to the group	
`awplus(config)#` `vlan classifier group 1 add rule 1`	Add VLAN classifier rule `1` to VLAN classifier group `1`.
`awplus(config)#` `vlan classifier group 1 add rule 2`	Add VLAN classifier rule `2` to VLAN classifier group `1`.
Step 4. Associate the created VLAN classifier group 1 with port1.0.1	
`awplus(config)#` `interface port1.0.1`	Enter Interface Configuration mode for `port1.0.1`.
`awplus(config-if)#` `vlan classifier activate 1`	Associate VLAN classifier group `1` with `port1.0.1`.
`awplus(config-if)#` `exit`	Exit Interface Configuration mode.
Step 5. Add VLAN 100 to be trunked over port1.0.2	

Table 16-5: Configuration procedure for Switch A(cont.)

Command	Description
`awplus(config)#` `interface port1.0.2`	Enter Interface Configuration mode for `port1.0.2`.
`awplus(config-if)#` `switchport mode trunk`	Enable switchport trunking on `port1.0.2`.
`awplus(config-if)#` `switchport trunk allowed vlan add 100`	Add VLAN 100 to be trunked over `port1.0.2`.
`awplus(config-if)#` `exit`	Exit Interface Configuration mode.
Step 6. Add VLAN 101 to be trunked over port1.0.3	
`awplus(config)#` `interface port1.0.3`	Enter Interface Configuration mode for `port1.0.3`.
`awplus(config-if)#` `switchport mode trunk`	Enable switchport trunking on `port1.0.3`.
`awplus(config-if)#` `switchport trunk allowed vlan add 101`	Add VLAN 101 to be trunked over `port1.0.3`.
`awplus(config-if)#` `exit`	Exit Interface Configuration mode.

Chapter 17: VLAN Commands

Command List 17.2
port-vlan-forwarding-priority 17.3
private-vlan 17.6
private-vlan association 17.7
show port-vlan-forwarding-priority 17.8
show vlan 17.9
show vlan classifier group 17.10
show vlan classifier group interface 17.11
show vlan classifier interface group 17.12
show vlan classifier rule 17.13
switchport access vlan 17.14
switchport enable vlan 17.15
switchport mode access 17.16
switchport mode private-vlan 17.17
switchport mode private-vlan trunk promiscuous 17.18
switchport mode private-vlan trunk secondary 17.20
switchport mode trunk 17.22
switchport private-vlan host-association 17.23
switchport private-vlan mapping 17.24
switchport trunk allowed vlan 17.25
switchport trunk native vlan 17.28
switchport voice dscp 17.29
switchport voice vlan 17.30
switchport voice vlan priority 17.32
vlan 17.33
vlan classifier activate 17.34
vlan classifier group 17.35
vlan classifier rule ipv4 ..... 17.36
vlan classifier rule proto 17.37
vlan database 17.40

Command List

This chapter provides an alphabetical reference of commands used to configure VLANs. For more information see **Chapter 16, VLAN Introduction**.

port-vlan-forwarding-priority

Use this command to set the highest priority protocol to control transitions from blocking to forwarding traffic. This command prioritizes switch port forwarding mode control, when more than one of EPSR, Loop Protection, and MAC thrashing protection protocols are used on the switch.

EPSR, Loop Protection and MAC Thrashing use the same mechanism to block or forward traffic. This command sets the highest priority protocol to control transitions from blocking to forwarding traffic. Setting the priority stops contention between protocols.

For example, If EPSR is set to the highest priority protocol to block traffic on vlan10 on port1.0.2 then this stops MAC Thrashing from forwarding traffic on vlan10 on port1.0.2.

Caution **loop-protection** and **none** parameter options must not be set on an EPSR master node. Use the **epsr** parameter option on an EPSR master node instead. Setting this command incorrectly on an EPSR master node could cause unexpected broadcast storms.

Use the **no** variant of this command to restore the default highest priority protocol back to the default of EPSR.

For more information about EPSR, see the section **"EPSR Introduction and Configuration" on page 57.1**.

Syntax

```
port-vlan-forwarding-priority {epsr|loop-protection|none}
no port-vlan-forwarding-priority
```

Parameter	Description
`epsr`	Sets EPSR as the highest priority protocol. Use this parameter on an EPSR master node to avoid unexpected broadcast storms.
`loop-protection`	Sets Loop Protection as the highest priority protocol. Note that this option must not be set on an EPSR master node. Use the **epsr** parameter option on an EPSR master node to avoid unexpected broadcast storms.
`none`	Sets the protocols to have equal priority. This was the previous behavior before this command was added, and allows protocols to override each other to set a port to forwarding a VLAN. Note that this option must not be set on a EPSR master node. Use the **epsr** parameter option on an EPSR master node to avoid unexpected broadcast storms.

Default By default, the highest priority protocol is EPSR

Mode Global Configuration

Usage EPSR, Loop Protection and MAC Thrashing protection do not usually need to be configured on a switch, because they perform similar functions—each prevents network loops by blocking a selected port for each (loop containing) VLAN.

However, if more than one of these three features is configured on a switch, you can use this command to prioritize either EPSR or Loop Protection when their effects on a port would conflict and override each other. Previously, each protocol could set a port to forwarding for a VLAN, sometimes overriding the previous setting by another protocol to block the port. This could sometimes lead to unexpected broadcast storms.

Now, when a protocol is set to have the highest priority over a data VLAN on a port, it will not allow other protocols to put that port-vlan into a forwarding state if the highest priority protocol blocked it.

The priority mechanism is only used for blocking-to-forwarding transitions; protocols remain independent on the forwarding-to-blocking transitions.

For example, with an EPSR master node in a two-node ESPR ring with the below settings:

- The EPSR master node primary port is configured to switchport interface **port1.0.1**
- The EPSR master node secondary port is configured to switchport interface **port1.0.2**
- The EPSR master node control VLAN is configured to VLAN interface **vlan10**
- The EPSR master node has a first data VLAN configured to VLAN interface **vlan20**
- The EPSR master node has a second data VLAN configured to VLAN interface **vlan30**.

Initially, the EPSR ring is complete, with **port1.0.2** blocking data VLANs **vlan20** and **vlan30** and some broadcast traffic flowing through. If the user removes **vlan30** from EPSR, a storm is created on **vlan30**. MAC thrashing protection detects it and blocks **vlan30**.

Then after the storm has stopped, MAC thrashing protection sets it to forwarding again and it keeps oscillating between forwarding and blocking. In the meantime, the user adds back **vlan30** to EPSR as a data VLAN and EPSR blocks it on **port1.0.2**.

If the priority is set to none (**port-vlan-forwarding-priority none**), MAC thrashing protection notices that the storm has stopped again and decides to put **vlan30** on **port1.0.2** into forwarding state. This overrides what EPSR requires for this port-VLAN and creates a storm. This matches the old behavior before this feature was implemented.

If the priority is set to EPSR or default (**port-vlan-forwarding-priority epsr**), MAC thrashing protection notices that the storm has stopped again and attempts to put **vlan30** on **port1.0.2** into forwarding state. The higher priority protocol (EPSR) is blocking the VLAN on this port, so it stays blocking and no storm occurs.

Example To prioritize EPSR over Loop Protection or MAC Thrashing protection settings, so that Loop Protection or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if EPSR has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority epsr
```

To prioritize Loop Protection over EPSR or MAC Thrashing protection settings, so that EPSR or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if Loop Protection has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority loop-
protection
```

To set EPSR, Loop Protection, and MAC Thrashing protection protocols to have equal priority for port forwarding and blocking, which allows the protocols to override each other to set a port to the forwarding or blocking states, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority none
```

To restore the default highest priority protocol back to the default of EPSR, use the commands:

```
awplus# configure terminal
awplus(config)# no port-vlan-forwarding-priority
```

Related Commands **show port-vlan-forwarding-priority**

private-vlan

Use this command to a create a private VLAN. Private VLANs can be either primary or secondary. Secondary VLANs can be ether community or isolated.

Use the **no** variant of this command to remove the specified private VLAN.

For more information, see the section **"Private VLANs" on page 16.5**.

Syntax

```
private-vlan <vlan-id> {community|isolated|primary}
no private-vlan <vlan-id> {community|isolated|primary}
```

Parameter	Description
<vlan-id>	VLAN ID in the range <2-4094> for the VLAN which is to be made a private VLAN.
`community`	Community VLAN.
`isolated`	Isolated VLAN.
`primary`	Primary VLAN.

Mode VLAN Configuration

Examples

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name vlan2 state enable
awplus(config-vlan)# vlan 3 name vlan3 state enable
awplus(config-vlan)# vlan 4 name vlan4 state enable
awplus(config-vlan)# private-vlan 2 primary
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 community
```

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 primary
awplus(config-vlan)# no private-vlan 3 isolated
awplus(config-vlan)# no private-vlan 4 community
```

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the **no** variant of this command to remove association of all the secondary VLANs to a primary VLAN.

For more information, see the section **"Private VLANs" on page 16.5**.

Syntax

```
private-vlan <primary-vlan-id> association {add <secondary-vlan-id>|
    remove <secondary-vlan-id>}

no private-vlan <primary-vlan-id> association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode VLAN Configuration

Examples The following commands associate primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association add 3
```

The following commands remove the association of primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association remove 3
```

The following commands remove all secondary VLAN associations of primary VLAN 2:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 association
```

show port-vlan-forwarding-priority

Use this command to display the highest priority protocol that controls port-vlan forwarding or blocking traffic. This command displays whether EPSR or Loop Protection is set as the highest priority for determining whether a port forwards a VLAN, as set by the **port-vlan-forwarding-priority** command.

For more information about EPSR, see the section **"EPSR Introduction and Configuration" on page 57.1**.

Syntax

```
show port-vlan-forwarding-priority
```

Mode

Privileged Exec

Example

To display the highest priority protocol, use the command:

```
awplus# show port-vlan-forwarding-priority
```

Output

Figure 17-1: Example output from the show port-vlan-forwarding-priority command

```
Port-vlan Forwarding Priority: EPSR
```

Related Commands

port-vlan-forwarding-priority

show vlan

Use this command to display information about a particular VLAN by specifying the VLAN ID. It displays information for all the VLANs configured.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show vlan {all|brief|dynamic|static|auto|static-ports<1-4094>}`

Parameter	Description
<1-4094>	Display information about the VLAN specified by the VLAN ID.
`all`	Display information about all VLANs on the device.
`brief`	Display information about all VLANs on the device.
`dynamic`	Display information about all VLANs learned dynamically.
`static`	Display information about all statically configured VLANs.
`auto`	Display information about all auto-configured VLANs.
`static-ports`	Display static egress/forbidden ports.

Mode User Exec and Privileged Exec

Example To display information about VLAN 2, use the command:

```
awplus# show vlan 2
```

Output **Figure 17-2: Example output from the show vlan command**

```
VLAN ID  Name            Type    State   Member ports
                                         (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ====================================
2       VLAN0002         STATIC  ACTIVE  port1.0.3(u) port1.0.4(u) port1.0.5(u)
                                         port1.0.6(u)
.
.
```

Related Commands **vlan**

show vlan classifier group

Use this command to display information about all configured VLAN classifier groups or a specific group.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show vlan classifier group [<1-16>]`

Parameter	Description
<1-16>	VLAN classifier group identifier

Mode User Exec and Privileged Exec

Usage If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

Example To display information about VLAN classifier group 1, enter the command:

```
awplus# show vlan classifier group 1
```

Related Commands **vlan classifier group**

show vlan classifier group interface

Use this command to display information about a single switch port interface for all configured VLAN classifier groups.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show vlan classifier group interface <switch-port>`

Parameter	Description
<switch-port>	Specify the switch port interface classifier group identifier

Mode User Exec and Privileged Exec

Usage All configured VLAN classifier groups are shown for a single interface.

Example To display VLAN classifier group information for switch port interface `port1.0.2`, enter the command:

```
awplus# show vlan classifier group interface port1.0.2
```

Output **Figure 17-3: Example output from the show vlan classifier group interface port1.0.1 command:**

```
vlan classifier group 1 interface port1.0.1
```

Related Commands **vlan classifier group**
show vlan classifier interface group

show vlan classifier interface group

Use this command to display information about all interfaces configured for a VLAN group or all the groups.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show vlan classifier interface group [<1-16>]`

Parameter	Description
<1-16>	VLAN classifier interface group identifier

Mode User Exec and Privileged Exec

Usage If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

Example To display information about all interfaces configured for all VLAN groups, enter the command:

```
awplus# show vlan classifier interface group
```

To display information about all interfaces configured for VLAN group 1, enter the command:

```
awplus# show vlan classifier interface group 1
```

Output **Figure 17-4: Example output from the show vlan classifier interface group command**

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
vlan classifier group 2 interface port1.0.3
vlan classifier group 2 interface port1.0.4
```

Output **Figure 17-5: Example output from the show vlan classifier interface group 1 command**

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
```

Related Commands **vlan classifier group**
show vlan classifier group interface

show vlan classifier rule

Use this command to display information about all configured VLAN classifier rules or a specific rule.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show vlan classifier rule [<1-256>]
```

Parameter	Description
<1-256>	VLAN classifier rule identifier

Mode User Exec and Privileged Exec

Usage If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

Example To display information about VLAN classifier rule 1, enter the command:

```
awplus# show vlan classifier rule 1
```

Output **Figure 17-6: Example output from the show vlan classifier rule 1 command**

```
vlan classifier group 1 add rule 1
```

Related Commands

vlan classifier activate
vlan classifier rule ipv4
vlan classifier rule proto

switchport access vlan

Use this command to change the port-based VLAN of the current port.

Use the **no** variant of this command to change the port-based VLAN of this port to the default VLAN, *vlan1*.

Syntax

```
switchport access vlan <vlan-id>
no switchport access vlan
```

Parameter	Description
<vlan-id>	<1-4094> The port-based VLAN ID for the port.

Default Reset the default VLAN 1 to specified switchports using the negated form of this command.

Mode Interface Configuration

Usage Any untagged frame received on this port will be associated with the specified VLAN.

Examples To change the port-based VLAN to VLAN 3 for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 3
```

To reset the port-based VLAN to the default VLAN 1 for `port1.0.2`, use the commands:

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

Related Commands show vlan

switchport enable vlan

This command enables the VLAN on the port manually once disabled by certain actions, such as QSP (QoS Storm Protection) or EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

Syntax `switchport enable vlan [<1-4094>]`

Parameter	Description
`vlan`	Re-enables the VLAN on the port.
<1-4094>	VLAN ID.

Mode Interface Configuration

Example To re-enable the `port1.0.1` from VLAN 1:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport enable vlan 1
```

Related Commands **show mls qos interface storm-status**
storm-window

switchport mode access

Use this command to set the switching characteristics of the port to access mode. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax `switchport mode access [ingress-filter {enable|disable}]`

Parameter	Description
`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode with ingress filtering on.

Usage Use access mode to send untagged frames only.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access ingress-filter
enable
```

switchport mode private-vlan

Use this command to make a Layer 2 port a private VLAN host port or a promiscuous port.

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

Syntax

```
switchport mode private-vlan {host|promiscuous}
no switchport mode private-vlan {host|promiscuous}
```

Parameter	Description
`host`	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
`promiscuous`	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode private-vlan host
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode private-vlan promiscuous
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport mode private-vlan promiscuous
```

Related Commands switchport private-vlan mapping

switchport mode private-vlan trunk promiscuous

Use this command to enable a port in trunk mode to be promiscuous port for isolated VLANs.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

Use the **no** variant of this command to remove a port in trunk mode as a promiscuous port for isolated VLANs. You must first remove the secondary port, or ports, in trunk mode associated with the promiscuous port with the **no switchport mode private-vlan trunk secondary** command.

Syntax

```
switchport mode private-vlan trunk promiscuous group <group-id>
no switchport mode private-vlan trunk promiscuous
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate the promiscuous port with secondary ports.

Default By default, a port in trunk mode is disabled as a promiscuous port.

Mode Interface Configuration

Usage A port must be put in trunk mode with **switchport mode trunk** command before it can be enabled as a promiscuous port.

To add VLANs to be trunked over the promiscuous port, use the **switchport trunk allowed vlan** command. These VLANs can be isolated VLANs, or non-private VLANs.

To configure the native VLAN for the promiscuous port, use the **switchport trunk native vlan** command. The native VLAN can be an isolated VLAN, or a non-private VLAN.

When you enable a promiscuous port, all of the secondary port VLANs associated with the promiscuous port via the group ID number must be added to the promiscuous port. In other words, the set of VLANs on the promiscuous port must be a superset of all the VLANs on the secondary ports within the group.

For further information, see **"Private VLANs for Trunked Ports" on page 16.11**.

Examples To create the isolated VLANs 2, 3 and 4 and then enable `port1.0.2` in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2-4
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2-4
awplus(config-if)# switchport mode private-vlan trunk
promiscuous group 3
```

To remove port1.0.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport mode private-vlan trunk
promiscuous
```

Note that you must remove the secondary port or ports enabled as trunk ports that are associated with the promiscuous port before removing the promiscuous port.

Related Commands
switchport mode private-vlan trunk secondary
switchport mode trunk
switchport trunk allowed vlan
switchport trunk native vlan

switchport mode private-vlan trunk secondary

Use this command to enable a port in trunk mode to be a secondary port for isolated VLANs.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

Use the **no** variant of this command to remove a port in trunk mode as a secondary port for isolated VLANs.

Syntax

```
switchport mode private-vlan trunk secondary group <group-id>
no switchport mode private-vlan trunk secondary
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate a secondary port with its promiscuous port.

Default By default, a port in trunk mode is disabled as a secondary port.

When a port in trunk mode is enabled to be a secondary port for isolated VLANs, by default it will have a native VLAN of **none** (no native VLAN specified).

Mode Interface Configuration

Usage A port must be put in trunk mode with **switchport mode trunk** command before the port is enabled as a secondary port in trunk mode.

To add VLANs to be trunked over the secondary port use the **switchport trunk allowed vlan** command. These must be isolated VLANs and must exist on the associated promiscuous port.

To configure the native VLAN for the secondary port, use the **switchport trunk native vlan** command. The native VLAN must be an isolated VLAN and must exist on the associated promiscuous port.

For further information, see **"Private VLANs for Trunked Ports" on page 16.11**.

Examples To create isolated private VLAN 2 and then enable `port1.0.3` in trunk mode as a secondary port for the this VLAN with the group ID of `3`, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2
awplus(config-if)# switchport mode private-vlan trunk
secondary group 3
```

To remove port1.0.3 in trunk mode as a secondary port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan trunk
secondary
```

Related Commands
switchport mode private-vlan trunk promiscuous
switchport mode trunk
switchport trunk allowed vlan
switchport trunk native vlan

switchport mode trunk

Use this command to set the switching characteristics of the port to trunk. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax `switchport mode trunk [ingress-filter {enable|disable}]`

Parameter	Description
`ingress-filter`	Set the ingress filtering for the frames received.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode, are untagged members of the default VLAN (vlan1), and have ingress filtering on.

Mode Interface Configuration

Usage A port in trunk mode can be a tagged member of multiple VLANs, and an untagged member of one native VLAN.

To configure which VLANs this port will trunk for, use the **switchport trunk allowed vlan** command.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk ingress-filter enable
```

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the **no** variant of this command to remove the association.

Syntax

```
switchport private-vlan host-association <primary-vlan-id> add
   <secondary-vlan-id>
no switchport private-vlan host-association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan host-association 2
add 3

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport private-vlan host-association
```

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the **no** variant of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Syntax

```
switchport private-vlan mapping <primary-vlan-id> add
   <secondary-vid-list>

switchport private-vlan mapping <primary-vlan-id> remove
   <secondary-vid-list>

no switchport private-vlan mapping
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vid-list>	VLAN ID of the secondary VLAN (either isolated or community), or a range of VLANs, or a comma-separated list of VLANs and ranges.

Mode Interface Configuration

Usage This command can be applied to a switch port or a static channel group, but not a dynamic (LACP) channel group. LACP channel groups (dynamic/LACP aggregators) cannot be promiscuous ports in private VLANs.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan mapping 2 add 3-4
awplus(config-if)# switchport private-vlan mapping 2 remove 3-4
awplus(config-if)# no switchport private-vlan mapping
```

Related Commands switchport mode private-vlan

switchport trunk allowed vlan

Use this command to add VLANs to be trunked over this switch port. Traffic for these VLANs can be sent and received on the port.

Use the **no** variant of this command to reset switching characteristics of a specified interface to negate a trunked configuration specified with **switchport trunk allowed vlan** command.

Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add <vid-list>
switchport trunk allowed vlan remove <vid-list>
switchport trunk allowed vlan except <vid-list>
no switchport trunk
```

Parameter	Description
`all`	Allow all VLANs to transmit and receive through the port.
`none`	Allow no VLANs to transmit and receive through the port.
`add`	Add a VLAN to transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
`remove`	Remove a VLAN from transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
`except`	All VLANs, except the VLAN for which the VID is specified, are part of its port member set. Only use this parameter to remove VLANs after either this parameter or the **all** parameter have added VLANs to a port.
<vid-list>	<2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the port. A single VLAN, VLAN range, or comma-separated VLAN list can be set. For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen. For a VLAN list, specify the VLAN numbers separated by commas. Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Default By default, ports are untagged members of the default VLAN (vlan1).

Mode Interface Configuration

Usage The **all** parameter sets the port to be a tagged member of all the VLANs configured on the device. The **none** parameter removes all VLANs from the port's tagged member set. The **add** and **remove** parameters will add and remove VLANs to and from the port's member set. See the note below about restrictions when using the **add**, **remove**, **except**, and **all** parameters.

Note: Only use the **add** or the **remove** parameters with this command if a list of VLANs are configured on a port. Only use the **except** parameter to remove VLANs after either the **except** or the **all** parameters have first been used to add a list of VLANs to a port.

Remove VLAN 3 by re-entering the **except** parameter with the list of VLANs to remove, instead of using the **remove** parameter, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3,4
```

Then the configuration is changed after entering the above commands to remove VLAN 3:

```
awplus#show running-config
!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-4
```

To add a VLAN, where the configuration for `port1.0.6` shows the below output:

```
awplus#show running-config
!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-5
```

Add VLAN 4 by re-entering the **except** parameter with a list of VLANs to exclude, instead of using the **add** parameter to include VLAN 4, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport trunk allowed vlan except 3,5
```

The configuration is changed after entering the above commands to add VLAN 4:

```
awplus#show running-config
!
interface port1.0.5
switchport
switchport mode trunk
switchport trunk allowed vlan except 3,5
```

Examples The following shows adding a single VLAN to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2,3,4
```

switchport trunk native vlan

Use this command to configure the native VLAN for this port. The native VLAN is used for classifying the incoming untagged packets. Use the **none** parameter with this command to remove the native VLAN from the port and set the acceptable frame types to vlan-tagged only.

Use the **no** variant of this command to revert the native VLAN to the default VLAN ID 1. Command negation removes tagged VLANs, and sets the native VLAN to the default VLAN.

Syntax

```
switchport trunk native vlan {<vid>|none}
no switchport trunk native vlan
```

Parameter	Description
`<vid>`	`<2-4094>` The ID of the VLAN that will be used to classify the incoming untagged packets. The VLAN ID must be a part of the VLAN member set of the port.
`none`	No native VLAN specified. This option removes the native VLAN from the port and sets the acceptable frame types to vlan-tagged only. Note: Use the **no** variant of this command to revert to the default VLAN 1 as the native VLAN for the specified interface switchport - not **none**.

Default VLAN 1 (the default VLAN), which is reverted to using the **no** form of this command.

Mode Interface Configuration

Examples The following commands show configuration of VLAN 2 as the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan 2
```

The following commands show the removal of the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan none
```

The following commands revert the native VLAN to the default VLAN 1 for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport trunk native vlan
```

switchport voice dscp

Use this command to configure the Layer 3 DSCP value advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified DSCP value.

Use the **no** variant of this command to reset the DSCP value to the default, 0.

Syntax

```
switchport voice dscp <0-63>
no switchport voice dscp
```

Parameter	Description
`dscp`	Specify a DSCP value for voice data.
<0-63>	DSCP value.

Default A DSCP value of 0 will be advertised.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (**lldp run** command on page 70.16)
- Voice VLAN is configured for the port (**switchport voice vlan** command on page 17.30)
- The port is configured to transmit LLDP advertisements—enabled by default (**lldp transmit receive** command on page 70.20)
- The port is configured to transmit Network Policy TLVs—enabled by default (**lldp med-tlv-select** command on page 70.9)
- There is an LLDP-MED device connected to the port

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice dscp 27
```

Related Commands

lldp med-tlv-select
show lldp
switchport voice vlan

switchport voice vlan

Use this command to configure the Voice VLAN tagging advertised when the transmission of LLDP-MED Network Policy TLVs for voice endpoint devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified tagging. This command also sets the ports to be spanning tree edge ports, that is, it enables spanning tree portfast on the ports.

Use the **no** variant of this command to remove LLDP-MED network policy configuration for voice devices connected to these ports. This does not change the spanning tree edge port status.

Syntax

```
switchport voice vlan [<vid>|dot1p|dynamic|untagged]
no switchport voice vlan
```

Parameter	Description
`<vid>`	VLAN identifier, in the range 1 to 4094.
`dot1p`	The IP phone should send User Priority tagged packets, that is, packets in which the tag contains a User Priority value, and a VID of 0. (The User Priority tag is also known as the 802.1p priority tag, or the Class of Service (CoS) tag.)
`dynamic`	The VLAN ID with which the IP phone should send tagged packets will be assigned by RADIUS authentication.
`untagged`	The IP phone should send untagged packets.

Default By default, no Voice VLAN is configured, and therefore no network policy is advertised for voice devices.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (**lldp run** command on page 70.16)
- Voice VLAN is configured for the port using this command (**switchport voice vlan**)
- The port is configured to transmit LLDP advertisements—enabled by default (**lldp transmit receive** command on page 70.20)
- The port is configured to transmit Network Policy TLVs—enabled by default (**lldp med-tlv-select** command on page 70.9)
- There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the **switchport voice vlan priority** command on page 17.32.

If the Voice VLAN details are to be assigned by RADIUS, then the RADIUS server must be configured to send the attribute “Egress-VLANID (56)” or “Egress-VLAN-Name (58)” in the RADIUS Accept message when authenticating a phone attached to this port.

For more information about configuring authentication for Voice VLAN, **“Configuring LLDP” on page 69.11**.

If the ports have been set to be edge ports by the **switchport voice vlan** command, the **no** variant of this command will leave them unchanged as edge ports. To set them back to

their default non-edge port configuration, use the **spanning-tree edgeport (RSTP and MSTP)** command on page 19.39.

Examples To tell IP phones connected to `port1.0.5` to send voice data tagged for VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice vlan 10
```

To tell IP phones connected to ports 1.0.2-1.0.6 to send priority tagged packets (802.1p priority tagged with VID 0, so that they will be assigned to the port VLAN) use the following commands. The priority value is 5 by default, but can be configured with the **switchport voice vlan priority** command.

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.6
awplus(config-if)# switchport voice vlan dot1p
```

To dynamically configure the VLAN ID advertised to IP phones connected to `port1.0.1` based on the VLAN assigned by RADIUS authentication (with RADIUS attribute "Egress-VLANID" or "Egress-VLAN-Name" in the RADIUS accept packet), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport voice vlan dynamic
```

To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on `port1.0.6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

Related Commands

lldp med-tlv-select
spanning-tree edgeport (RSTP and MSTP)
switchport voice dscp
switchport voice vlan priority
show lldp

switchport voice vlan priority

Use this command to configure the Layer 2 user priority advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. This is the priority in the User Priority field of the IEEE 802.1Q VLAN tag, also known as the Class of Service (CoS), or 802.1p priority. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified priority.

Syntax

```
switchport voice vlan priority <0-7>
no switchport voice vlan priority
```

Parameter	Description
`priority`	Specify a user priority value for voice data.
<0-7>	Priority value.

Default By default, the Voice VLAN user priority value is 5.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (**lldp run** command on page 70.16)
- Voice VLAN is configured for the port (**switchport voice vlan** command on page 17.30)
- The port is configured to transmit LLDP advertisements—enabled by default (**lldp transmit receive** command on page 70.20)
- The port is configured to transmit Network Policy TLVs—enabled by default (**lldp med-tlv-select** command on page 70.9)
- There is an LLDP-MED device connected to the port.

To set the Voice VLAN tagging to be advertised, use the **switchport voice vlan** command on page 17.30.

Example To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on `port1.0.6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

Related Commands

lldp med-tlv-select
show lldp
switchport voice vlan

vlan

This command creates VLANs, assigns names to them, and enables or disables them. Specifying the `disable` state causes all forwarding over the specified VLAN ID to cease. Specifying the `enable` state allows forwarding of frames on the specified VLAN.

The **no** variant of this command destroys the specified VLANs.

Syntax

```
vlan <vid> [name <vlan-name>] [state {enable|disable}]
vlan <vid-range> [state {enable|disable}]
vlan {<vid>|<vlan-name>} [mtu <mtu-value>]
no vlan {<vid>|<vid-range>} [mtu]
```

Parameter	Description
<vid>	The VID of the VLAN to enable or disable in the range <**1-4094**>.
<vlan-name>	The ASCII name of the VLAN. Maximum length: **32** characters.
<vid-range>	Specifies a range of VLAN identifiers.
<mtu-value>	Specifies the Maximum Transmission Unit (MTU) size in bytes, in the range 68 to1500 bytes, for the VLAN.
`enable`	Sets VLAN into an `enable` state.
`disable`	Sets VLAN into a `disable` state.

Default By default, VLANs are enabled when they are created.

Mode VLAN Configuration

Examples

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 45 name accounts state enable
```

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 45
```

Related Commands **mtu**
vlan database
show vlan

vlan classifier activate

Use this command in Interface Configuration mode to associate a VLAN classifier group with the switch port.

Use the **no** variant of this command to remove the VLAN classifier group from the switch port.

Syntax

```
vlan classifier activate <vlan-class-group-id>
no vlan classifier activate <vlan-class-group-id>
```

Parameter	Description
<vlan-class-group-id>	Specify a VLAN classifier group identifier in the range <1-16>.

Mode Interface Configuration mode for a switch port.

Usage See the **Protocol Based VLAN Configuration Example** section in **Chapter 16, VLAN Introduction** for a configuration example and network topology using this command.

Example To associate VLAN classifier group 3 with switch `port1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# vlan classifier activate 3
```

To remove VLAN classifier group 3 from switch `port1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no vlan classifier activate 3
```

Related Commands

show vlan classifier rule
vlan classifier group
vlan classifier rule ipv4
vlan classifier rule proto

vlan classifier group

Use this command to create a group of VLAN classifier rules. The rules must already have been created.

Use the **no** variant of this command to delete a group of VLAN classifier rules.

Syntax

```
vlan classifier group <1-16> {add|delete} rule <vlan-class-rule-id>
no vlan classifier group <1-16>
```

Parameter	Description
<1-16>	VLAN classifier group identifier
add	Add the rule to the group.
delete	Delete the rule from the group.
<vlan-class-rule-id>	The VLAN classifier rule identifier.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# vlan classifier group 3 add rule 5
```

Related Commands

show vlan classifier rule
vlan classifier activate
vlan classifier rule ipv4
vlan classifier rule proto

vlan classifier rule ipv4

Use this command to create an IPv4 subnet-based VLAN classifier rule and map it to a specific VLAN. Use the **no** variant of this command to delete the VLAN classifier rule.

Syntax

```
vlan classifier rule <1-256> ipv4 <ip-addr/prefix-length>  vlan
   <1-4094>

no vlan classifier rule <1-256>
```

Parameter	Description
<1-256>	Specify the VLAN Classifier Rule identifier.
<ip-addr/prefix-length>	Specify the IP address and prefix length.
<1-4094>	Specify a VLAN ID to which an untagged packet is mapped in the range *<1-4094>*.

Mode Global Configuration

Usage If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

Example

```
awplus# configure terminal
awplus(config)# vlan classifier rule 3 ipv4 3.3.3.3/8 vlan 5
```

Related Commands

show vlan classifier rule
vlan classifier activate
vlan classifier rule proto

vlan classifier rule proto

Use this command to create a protocol type-based VLAN classifier rule, and map it to a specific VLAN. See the published IANA EtherType IEEE 802 numbers here:

www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt.

Instead of a protocol name the decimal value of the protocol's EtherType can be entered. The EtherType field is a two-octet field in an Ethernet frame. It is used to show which protocol is encapsulated in the payload of the Ethernet frame. Note that EtherTypes in the IANA 802 numbers are given as hexadecimal values.

The **no** variant of this command removes a previously set rule.

Syntax

```
vlan classifier rule <1-256> proto <protocol> encap {ethv2|nosnapllc|
    snapllc} vlan <1-4094>

no vlan classifier rule <1-256>
```

Parameter	Description	
<1-256>	VLAN Classifier identifier	
`proto`	Protocol type	
<protocol>	Specify a protocol either by its decimal number (0-65535) or by one of the following protocol names:	
	`[arp|2054]`	Address Resolution protocol
	`[atalkaarp|33011]`	Appletalk AARP protocol
	`[atalkddp|32923]`	Appletalk DDP protocol
	`[atmmulti|34892]`	MultiProtocol Over ATM protocol
	`[atmtransport|34948]`	Frame-based ATM Transport protocol
	`[dec|24576]`	DEC Assigned protocol
	`[deccustom|24582]`	DEC Customer use protocol
	`[decdiagnostics|24581]`	DEC Systems Comms Arch protocol
	`[decdnadumpload|24577]`	DEC DNA Dump/Load protocol
	`[decdnaremoteconsole|24578]`	DEC DNA Remote Console protocol
	`[decdnarouting|24579]`	DEC DNA Routing protocol
	`[declat|24580]`	DEC LAT protocol
	`[decsyscomm|24583]`	DEC Systems Comms Arch protocol

Parameter (cont.)	Description (cont.)	
	`[g8bpqx25|2303]`	G8BPQ AX.25 protocol
	`[ieeeaddrtrans|2561]`	Xerox IEEE802.3 PUP Address
	`[ieeepup|2560]`	Xerox IEEE802.3 PUP protocol
	`[ip|2048]`	IP protocol
	`[ipv6|34525]`	IPv6 protocol
	`[ipx|33079]`	IPX protocol
	`[netbeui|61680]`	IBM NETBIOS/NETBEUI protocol
	`[netbeui|61681]`	IBM NETBIOS/NETBEUI protocol
	`[pppdiscovery|34915]`	PPPoE discovery protocol
	`[pppsession|34916]`	PPPoE session protocol
	`[rarp|32821]`	Reverse Address Resolution protocol
	`[x25|2056]`	CCITT.25 protocol
	`[xeroxaddrtrans|513]`	Xerox PUP Address Translation protocol
	`[xeroxpup|512]`	Xerox PUP protocol
`ethv2`	Ethernet Version 2 encapsulation	
`nosnapllc`	LLC without SNAP encapsulation	
`snapllc`	LLC SNAP encapsulation	
`<1-4094>`	Specify a VLAN ID to which an untagged packet is mapped in the range *`<1-4094>`*	

Mode Global Configuration

Usage If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN. Ethernet Frame Numbers may be entered in place of the protocol names listed. For a full list please refer to the IANA list online: **www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt**

Examples

```
awplus# configure terminal
awplus(config)# vlan classifier rule 1 proto x25 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 2 proto 512 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 3 proto 2056 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 4 proto 2054 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 5 proto 34525 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 6 proto ipv6 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 7 proto 2048 encap ethv2
vlan 2
awplus(config)# vlan classifier rule 8 proto ip encap ethv2
vlan 2
```

Validation Output

```
awplus# show vlan classifier rule
```

```
vlan classifier rule 16 proto rarp encap ethv2 vlan 2
vlan classifier rule 8 proto encap ethv2 vlan 2
vlan classifier rule 4 proto arp encap ethv2 vlan 2
vlan classifier rule 3 proto xeroxpup encap ethv2 vlan 2
vlan classifier rule 2 proto ip encap ethv2 vlan 2
vlan classifier rule 1 proto ipv6 encap ethv2 vlan 2
```

Related Commands

show vlan classifier rule
vlan classifier activate
vlan classifier group

vlan database

Use this command to enter the VLAN Configuration mode.

Syntax `vlan database`

Mode Global Configuration

Usage Use this command to enter the VLAN configuration mode. You can then add or delete a VLAN, or modify its values.

Example In the following example, note the change to VLAN configuration mode from Configure mode:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)#
```

Related Commands vlan

Chapter 18: Spanning Tree Introduction: STP, RSTP, and MSTP

Introduction 18.2
Overview of Spanning Trees 18.2
- Spanning Tree Operation 18.2
- Spanning Tree Modes 18.4

Spanning Tree Protocol (STP) 18.5
Configuring STP 18.6
Rapid Spanning Tree Protocol (RSTP) 18.8
Configuring RSTP 18.9
Multiple Spanning Tree Protocol (MSTP) 18.11
- Multiple Spanning Tree Instances (MSTI) 18.12
- MSTP Regions 18.13
- Common and Internal Spanning Tree (CIST) 18.15
- MSTP Bridge Protocol Data Units (BPDUs) 18.17

Configuring MSTP 18.19

Introduction

This chapter describes and provides configuration procedures for:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

For detailed information about the commands used to configure spanning trees, see **Chapter 19, Spanning Tree Commands**.

Overview of Spanning Trees

The concept of the spanning tree protocol was devised to address broadcast storming. The spanning tree algorithm itself is defined by the IEEE standard 802.1D and its later revisions.

The IEEE Standard 802.1 uses the term “bridge” to define the spanning tree operation, and uses terms such as Bridge Protocol Data Units and Root Bridge when defining spanning tree protocol functions.

When a bridge receives a frame, it reads the source and destination address fields. The bridge then enters the frame’s source address in its forwarding database. In doing this the bridge associates the frame’s source address with the network attached to the port on which the frame was received. The bridge also reads the destination address and if it can find this address in its forwarding database, it forwards the frame to the appropriate port. If the bridge does not recognize the destination address, it forwards the frame out from all its ports except for the one on which the frame was received, and then waits for a reply. This process is known as “flooding”.

A significant problem arises where bridges connect via multiple paths. A frame that arrives with an unknown destination address is flooded over all available paths. The arrival of these frames at another network via different paths and bridges produces major problems. The bridges can become confused about the location of the send and receive devices and begin sending frames in the wrong directions. This process is self-perpetuating and produces a condition known as a broadcast storm, where the increase of circulating frames can eventually overload the network.

Spanning Tree Operation

Where a LAN’s topology results in more than one path existing between bridges, frames transmitted onto the extended LAN circulate in increasing numbers around the loop, decreasing performance and potentially overloading the network. However, multiple paths through the extended LAN are often required in order to provide redundancy and backup in the event of a bridge or link failure.

The spanning tree is created through the exchange of Bridge Protocol Data Units (BPDUs) between the bridges in the LAN. The spanning tree algorithm operates by:

- Automatically computing a loop-free portion of the topology, called a *spanning tree*. The topology is dynamically pruned to the spanning tree by declaring certain ports on a switch to be redundant, and placing them into a ‘blocking’ state.
- Automatically recovering from a switch failure that would partition the extended LAN by reconfiguring the spanning tree to use redundant paths, if available.

The logical tree computed by the spanning tree algorithm has the following properties:

- A single bridge is selected to become the spanning tree's unique *root bridge*. This is the device that advertises the lowest Bridge ID. Each bridge is uniquely identified by its Bridge ID, which comprises the bridge's *root priority* (a spanning tree parameter) followed by its MAC address.
- Each bridge or LAN in the tree, except the root bridge, has a unique parent, known as the *designated bridge*. Each LAN has a single bridge, called the *designated bridge*, that connects it to the next LAN on the path towards the root bridge.
- Each port connecting a bridge to a LAN has an associated *cost*, called the *root path cost*. This is the sum of the costs for each path between the particular bridge port and the root bridge. The designated bridge for a LAN is the one that advertises the lowest *root path cost*. If two bridges on the same LAN have the same lowest root path cost, then the switch with the lowest bridge ID becomes the designated bridge.

The spanning tree computation is a continuous, distributed process to establish and maintain a spanning tree (**Table 18-1**). The basic algorithm is similar for STP, RSTP and MSTP modes.

Table 18-1: Spanning tree process

The spanning tree algorithm ...	By ...
Selects a root bridge	It selects as the root bridge for the spanning tree the device with the (numerically) lowest bridge identifier (that is, the device with lowest root bridge priority value, or if they have the same priority, the bridge with the lowest MAC address).
Selects root ports	On each device, it selects the root port according to: ■ the port with the lowest path cost to the root bridge ■ the port connected to the bridge with the lowest root identifier ■ MSTP and RSTP only: the port with the lowest port priority value ■ the port with the lowest port number[1]
Blocks alternate ports	In order to prevent loops, it blocks alternate ports (discarding state) that provide higher cost paths to the root bridge.
Blocks backup ports	Where a second port connects one switch back to itself, it blocks the backup port that has the highest path cost or port number.
Selects designated ports	All other ports that are not disabled are selected as designated ports and are eventually made active (Forwarding state).
Maintains the spanning tree	If a switch or port fails, the spanning tree configures a new active topology, changing some port states, to reestablish connectivity and block loops. Depending on where the failure occurs, the changes may be widespread (e.g. if the root bridge fails), or local (e.g. if a designated port fails).

1. **The whole three part port number (D.M.P) is used to find the lowest port number, where D is the device number within a stack (1 for a non stacked device), M is the module number within the device (note that 0 is used for all base-board connected ports), and P is the number of the port within the base-board.**

The logical spanning tree, sometimes called the *active topology*, includes the root bridge and all designated bridges, meaning all ports that are to be used for communication within the spanning tree. These ports are in the forwarding state. Ports removed from the logical spanning tree are not in the forwarding state. To implement the spanning tree algorithm, devices communicate with one another using the Spanning Tree Protocol.

Spanning Tree Modes

STP can run in one of three modes: STP, RSTP or MSTP. A device running RSTP is compatible with other devices running STP; a device running MSTP is compatible with other devices running RSTP or STP. By default, on a device in MSTP mode each port automatically detects the mode of the device connected to it (MSTP, RSTP or STP), and responds in the appropriate mode by sending messages (BPDUs) in the corresponding format. Ports on a device in RSTP mode can automatically detect and respond to connected devices in RSTP and STP mode. Particular ports can also be forced to only operate in a particular mode (**spanning-tree force-version** command on page 19.44).

STP The Spanning Tree Protocol (STP) is the original protocol defined by IEEE standard 802.1D-1988. It creates a single spanning tree over a network.

STP mode may be useful for supporting applications and protocols whose frames may arrive out of sequence or duplicated, for example NetBeui.

RSTP Rapid Spanning Tree Protocol (RSTP) also creates a single spanning tree over a network. Compared with STP, RSTP provides for more rapid convergence to an active spanning tree topology. RSTP is defined in IEEE standard 802.1D-2004.

By default, the device operates in RSTP mode.

MSTP The Multiple Spanning Tree Protocol (MSTP) addresses the limitations in the previous spanning tree protocols, STP and RSTP, within networks that use multiple VLANs with topologies that employ alternative physical links. It supports multiple spanning tree instances on any given link within a network, and supports large networks by grouping bridges into regions that appear as a single bridge to other devices.

MSTP is defined in IEEE standard 802.1Q-2005. The protocol builds on, and remains compatible with, the previous IEEE standards defining STP and RSTP.

Spanning Tree Protocol (STP)

STP uses the process described in **Table 18-1** to avoid loops.

STP port states

In STP mode, each switch port can be in one of five spanning tree states, and one of two switch states. The state of a switch port is taken into account by STP. The STP port states (**Table 18-2**) affect the behavior of ports whose switch state is enabled.

Table 18-2: STP port states

State	Meaning
DISABLED	STP operations are disabled on the port. The port does not participate in the operation of the Spanning Tree Algorithm and Protocol. The port can still switch if its switch state is enabled.
BLOCKING	The forwarding process discards received frames and does not submit forwarded frames for transmission. This is the “standby” mode.The port does not participate in frame relay.
LISTENING	The port is enabled for receiving frames only. The port is preparing to participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.
LEARNING	The port is enabled for receiving frames only, and the Learning Process can add new source address information to the Forwarding Database.
FORWARDING	The normal state for a switch port. The forwarding process and the Spanning Tree entity are enabled for transmit and receive operations on the port.

Configuring STP

By default, RSTP is enabled on all switch ports. This section provides a procedure for configuring STP (**Table 18-3**).

To configure other modes, see **"Configuring RSTP" on page 18.9** or **"Configuring MSTP" on page 18.19**.

Table 18-3: Configuration procedure for STP

Command	Description
Step 1. Configure STP RSTP is enabled by default with default settings on all switch ports to prevent Layer 2 loops in your network.	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `spanning-tree mode stp`	By default, the device is in RSTP mode. Change to STP mode.
`awplus(config)#` `spanning-tree enable`	By default, spanning tree is enabled on all switch ports. If it has been disabled, enable it for STP.
`awplus(config)#` `spanning-tree priority <priority>`	By default, all devices have the same root bridge priority, 32768 (8000 in hexadecimal), so the device with the lowest MAC address becomes the root bridge. If you want the device to be the root bridge, set the root bridge priority to a value lower than 32768. Enter a value in the range 0 to 61440. If you enter a number that is not a multiple of 4096, the switch rounds the number down.
Step 2. Configure Root Guard 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).	
`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for the switch ports you want to enable Root Guard for.
`awplus(config-if)#` `spanning-tree guard root`	Enable the Guard Root feature for these ports.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `exit`	Return to Privileged Exec mode.

Table 18-3: Configuration procedure for STP(cont.)

Command	Description
Step 3. Check STP configuration	
`awplus#` `show spanning-tree [interface <port-list>]`	Display the spanning tree configuration for the device, and confirm the new root bridge priority (Bridge Priority). Note that the Bridge ID is in a form like this: 80000000cd240331, and that other IDs follow the same pattern. This is made up of: 8000—the devices' root bridge priority in hexadecimal 0000cd240331—the devices' MAC address.

Advanced configuration: For most networks the default settings for path costs will be suitable, however, you can configure them if required (**spanning-tree path-cost**).

Rapid Spanning Tree Protocol (RSTP)

RSTP uses the process described in **Table 18-1** to avoid loops.

A spanning tree running in STP mode can take up to one minute to rebuild after a topology or configuration change. The RSTP algorithm provides for a faster recovery of connectivity following the failure of a bridge, bridge port, or a LAN. RSTP provides rapid recovery by including port roles in the computation of port states, and by allowing neighboring bridges to explicitly acknowledge signals on a point-to-point link that indicate that a port wants to enter the forwarding mode.

In rapid mode, the rapid transition of a port to the forwarding state is possible when the port is considered to be part of a point-to-point link, or when the port is considered to be an *edge* port. An edge port is one that attaches to a LAN that has no other bridges attached.

Table 18-4: RSTP port states

State	Meaning
DISABLED	STP operations are disabled on the port.
DISCARDING	The port does not participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.
LEARNING	The port is enabled for receiving frames only, and the learning process can add new source address information to the forwarding database. The port does not forward any frames.
FORWARDING	The normal state for a switch port. The forwarding process and the Spanning Tree entity are enabled for transmit and receive operations on the port.

Configuring RSTP

RSTP is enabled by default with default settings on all switch ports to prevent Layer 2 loops in your network. No further configuration is required if you want to use RSTP with these default settings. For further RSTP configuration, see **Table 18-5** below.

To configure other modes, see **"Configuring MSTP" on page 18.19** or **"Configuring STP" on page 18.6**.

For detailed configuration examples, see the How To Note *How To Configure Basic Switching Functionality*, available from **alliedtelesis.com**.

Table 18-5: Configuration procedure for RSTP

Command	Description
Step 1. Configure RSTP RSTP is enabled by default with default settings on all switch ports to prevent Layer 2 loops in your network. No further configuration is required if you want to use RSTP with these default settings. If you need to restore the device to RSTP after it has been set to another mode, or modify the default RSTP settings, follow the procedure below.	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `spanning-tree mode rstp`	By default, the device is in RSTP mode. If it has been changed to STP or MSTP mode, change it back to RSTP.
`awplus(config)#` `spanning-tree enable`	By default, spanning tree is enabled on all switch ports. If it has been disabled, enable it for RSTP.
`awplus(config)#` `spanning-tree priority <priority>`	By default, all devices have the same root bridge priority, 32768 (8000 in hexadecimal), so the device with the lowest MAC address becomes the root bridge. If you want the device to be the root bridge, set the root bridge priority to a value lower than 32768. Enter a value in the range 0 to 61440. If you enter a number that is not a multiple of 4096, the switch rounds the number down.
Step 2. Configure edge ports If some switch ports are connected to devices that cannot generate BPDUs (such as workstations), you can set particular switch ports as edge ports, or set them to automatically detect whether they are edge ports.	
`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for these switch ports.

`awplus(config-if)#`
`spanning-tree edgeport (RSTP and MSTP)`
or
`awplus(config-if)#`
`spanning-tree autoedge (RSTP and MSTP)`
	Set these ports to be edge ports,
	or
	set these ports to automatically detect whether they are edge ports.

Table 18-5: Configuration procedure for RSTP(cont.)

Command	Description
Step 3. Configure Root Guard	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for the switch ports you want to enable Root Guard for.
`awplus(config-if)#` `spanning-tree guard root`	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). Enable the Guard Root feature if required.
Step 4. Configure BPDU Guard	
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `spanning-tree portfast bpdu-guard`	If required, enable the BPDU Guard feature.
`awplus(config)#` `spanning-tree errdisable-timeout enable`	Set a timeout for ports that are disabled due to the BPDU guard feature.
`awplus(config)#` `spanning-tree errdisable-timeout interval`	Specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.
Step 5. Check RSTP configuration	
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show spanning-tree [interface <port-list>]`	Display the spanning tree configuration for the device, and confirm the new root bridge priority (Bridge Priority). Note that the Bridge ID is in a form like this: 80000000cd240331, and that other IDs follow the same pattern. This is made up of: 8000—the devices' root bridge priority in hexadecimal 0000cd240331—the devices' MAC address.

Advanced configuration: For most networks the default settings for path costs will be suitable, however, you can configure them if required (**spanning-tree path-cost**).

Multiple Spanning Tree Protocol (MSTP)

Conceptually, MSTP views the total bridged network as one that comprises a number of *Multiple Spanning Tree Regions* (MSTRs), where each region can contain up to 64 spanning trees, which operate locally, called *Multiple Spanning Tree Instances* (MSTIs). AlliedWare Plus™ supports up to 15 MSTIs. The regions are linked by the *Common Internal Spanning Tree* (CIST).

MSTP uses BPDUs to exchange information between spanning-tree compatible devices, to prevent loops in each MSTI and also in the CIST, by selecting active and blocked paths. This process is described in **Table 18-1**.

If multiple ports are aggregated together into a dynamic (LACP) or static channel group, then the spanning-tree process is aware of the link aggregation and treats the aggregated ports as a single logical path.

Advantage of MSTP over RSTP

MSTP is similar to RSTP, in that it provides loop resolution and rapid convergence. However, RSTP can keep track of only one spanning-tree. MSTP can track many spanning-trees, referred to as *instances*. MSTP makes it possible to have different forwarding paths for different MST instances. This enables load balancing of network traffic across redundant links, so that all the links in a network can be used by at least one MSTI, and no link is left completely idle. That is to say that no link is unnecessarily shut down by spanning-tree.

Essentially, MSTP is VLAN aware and RSTP is not VLAN aware. MSTP BPDUs and RSTP BPDUs are compatible, so a network can have a mixture of MSTP and RSTP areas.

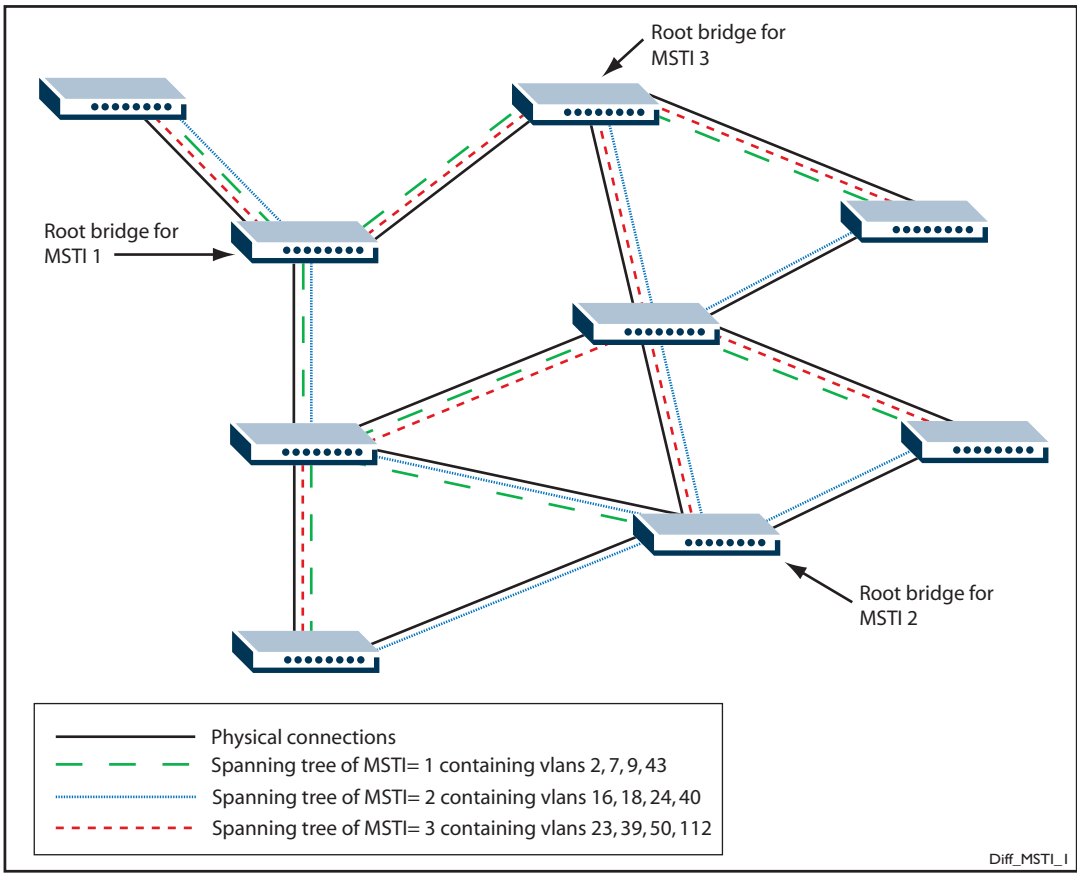
Multiple Spanning Tree Instances (MSTI)

MSTP enables the grouping and mapping of VLANs to different spanning tree instances. So, an MST Instance (MSTI) is a particular set of VLANs that are all using the same spanning tree.

In a network where all VLANs span all links of the network, judicious choice of bridge priorities for different MSTIs can result in different switches becoming root bridges for different MSTIs. That will result in the different MSTIs choosing different active topologies on the network. An example of how different MSTIs can choose different active topologies on the same physical set of links is illustrated in **Figure 18-1**.

MSTP is compatible with RSTP and STP—see **"Common and Internal Spanning Tree (CIST)" on page 18.15**.

Figure 18-1: Different spanning trees created by different MSTIs on the same physical layout



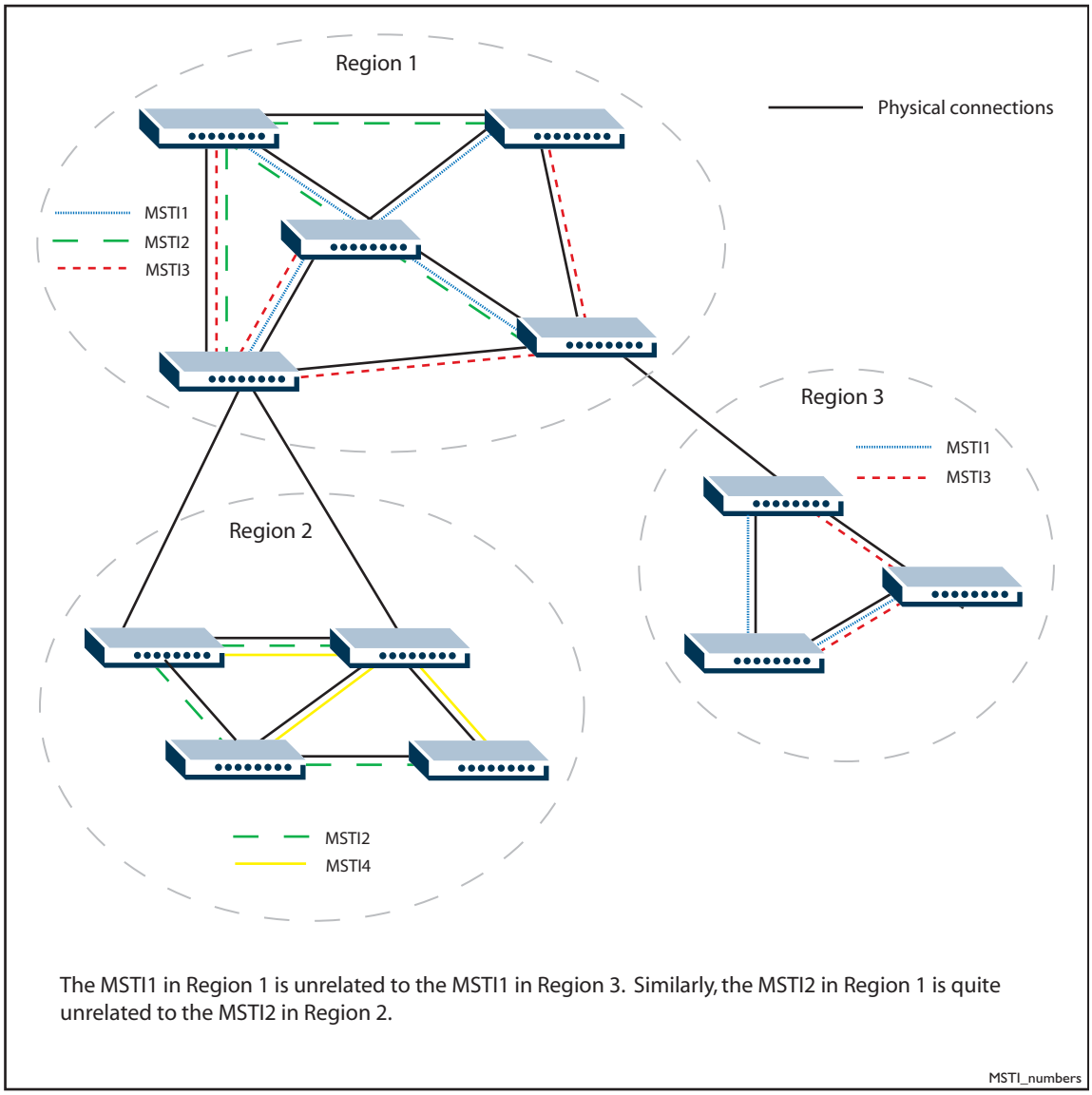
MSTP Regions

An MST region is a set of interconnected switches that all have the same values for the following MST configuration identification elements:

- MST configuration name - the name of the MST region
- Revision level - the revision number of configuration
- Configuration Digest - the mapping of which VLANs are mapped to which MST instances

Each of the MST instances created are identified by an MSTI number. This number is locally significant within the MST region. Therefore, an MSTI will not span across MST regions.

Figure 18-2: MSTIs in different regions



The task of assigning each bridge to a particular region is achieved by the member bridges each comparing their *MST Configuration Identifiers*. More information on configuration identifiers is provided in **Table 18-6**, but for the moment an *MST Configuration Identifier* can simply be thought of as an identifier that represents the mapping of VLANs to MSTIs within each bridge. Therefore, bridges with identical *MST Configuration Identifiers*, must have identical MSTI mapping tables.

While each MSTI can have multiple VLANs, each VLAN can be associated with only one MSTI. Once these associations have been made, the bridges in each region can transmit their spanning tree BPDUs and advertise their MSTIs. This in turn establishes the active data paths between the bridges for each group of VLANs (that is, for each MSTI) and block any duplicate paths within each instance. A particular advantage of this enhancement applies where a large number of VLANs share a few internetwork paths. In this situation there need only be as many Multiple Spanning Tree Instances (MSTIs) as there are source and destination bridge pairs, remembering that a pair of bridges probably has multiple paths between them.

In order to ensure that each bridge within a region maintains the same configuration information (particularly their VID to MSTI mappings) and to ensure each bridge's membership of a particular region, the bridges exchange configuration information in the form of *MST Configuration Identifiers*. **Table 18-6** provides a breakdown of an *MST Configuration Identifier*. A detailed explanation of bridge configuration identifiers can be found in Section 13.7 of the IEEE 802.1Q-2003 standard.

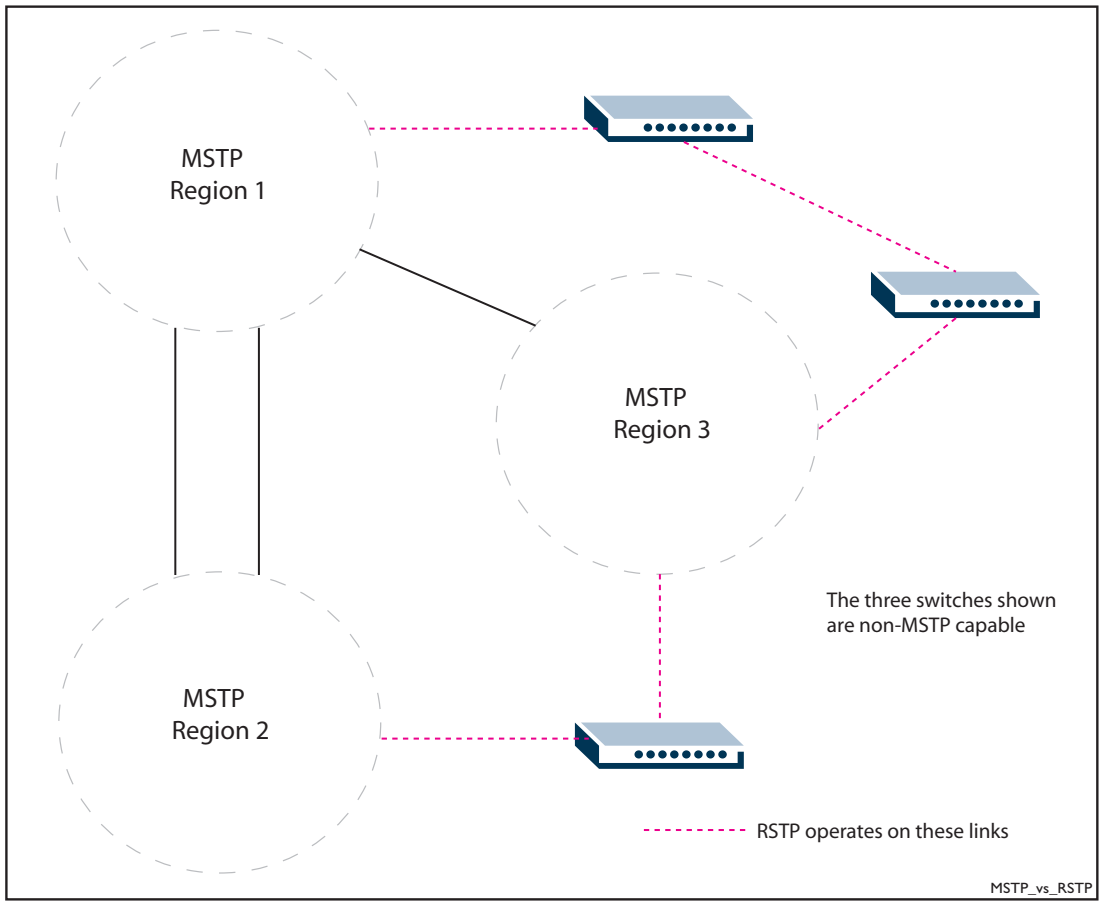
Table 18-6: MST Configuration Identifier

Field Name	Description
Format Selector	A single octet field whose value of 0 indicates MSTP operation
Region Name	A name (up to 32 characters long) that identifies a particular MST region, defined using the **region (MSTP)** command on page 19.11
Revision Level	A number representing the region's revision level, defined using the **revision (MSTP)** command on page 19.12.
Configuration Digest	A 16 octet (HMAC-MD5 based) signature created from the MST configuration table.

Common and Internal Spanning Tree (CIST)

The CIST is the default spanning tree instance of MSTP, i.e. all VLANs that are not members of particular MSTIs are members of the CIST. Also, an individual MST region can be regarded as a single virtual bridge by other MST regions. The spanning tree that runs between regions is the CIST. The CIST is also the spanning tree that runs between MST regions and Single Spanning Tree (SST) entities. So, in **Figure 18-3**, the STP that is running between the regions, and to the SST bridges, is the CIST.

Figure 18-3: The CIST operates on links between regions and to SST devices



Compatibility with Previous Spanning Tree Protocols

MSTP provides for compatibility with older spanning tree protocols in several ways. In addition to the MST region described in the previous section, the protocol provides for single spanning tree systems by employing a Common and Internal Spanning Tree (CIST). The CIST applies a common and internal spanning tree protocol to the whole of the bridged network and is a direct equivalent to the internal spanning tree (IST) protocol of earlier versions.

In common with legacy spanning tree systems, the CIST protocol first determines its root bridge from all the bridges on the network. This is the bridge that contains the lowest bridge identifier. The protocol then selects a regional root bridge for each MSTR. This is the bridge that provides the best path to the CIST root. After the MSTR root bridges have been chosen, they then act on the region's behalf in such a way that the region appears to the Common Spanning Tree (CST) as a virtual bridge. So in addition to having multiple MSTIs, each region operates as a bridge in a CST.

CIST In addition to the individual MSTIs within each MSTP region, the MSTP region is a member of a network-wide spanning tree called the Common and Internal Spanning Tree (CIST). Conceptually, each region represents a virtual bridge. Internal and external bridge connectivity are two independent functions.

Frames with VIDs allocated to the CIST are subject to the rules and path costs of the complete bridged LAN as determined by the CIST's vectors. Frames other than these are subject to the CIST when traveling outside their region, and subject to its particular MSTI inside the region.

The following operational rules apply:

- Each bridge can be a member of only one region.
- A data frame is associated with a single VID.
- Data frames with a given VID are associated with either the CIST or their particular MSTI, but not both.

The role of the Common Spanning Tree (CST) in a network, and the Common and Internal Spanning Tree (CIST) configured on each device, is to prevent loops within a wider network that may span more than one MSTP region and parts of the network running in legacy STP or RSTP mode.

CIST first allocates root and designated bridges by selecting the bridge with the lowest identifier as the root. MSTP then deals with any loops between the regions in the CST. It does this by considering the CIST "vectors" in the following order:

1. CIST External Root Path Cost
2. CIST Regional Root Identifier
3. CIST Internal Root Path Cost
4. CIST Designated Bridge Identifier
5. CIST Designated Port Identifier
6. CIST Receiving Port Identifier

MSTP Bridge Protocol Data Units (BPDUs)

The main function of bridge protocol data units is to enable MSTP to select its root bridges for the CIST (**"Common and Internal Spanning Tree (CIST)" on page 18.15**) and each MSTI. MSTP is compatible with earlier spanning tree versions; its Bridge Protocol Data Unit (BPDU) formats build on earlier versions (**"Compatibility with Previous Spanning Tree Protocols" on page 18.15**).

Table 18-7 shows the standardized format for MSTP BPDU messages. The general format of the BPDUs comprise a common generic portion—octets 1 to 36—that are based on those defined in IEEE Standard 802.1D, 1998, followed by components that are specific to CIST—octets 37 to 102. Components specific to each MSTI are added to this BPDU data block.

Table 18-7: MSTP Bridge Protocol Data Units (BPDUs)

Field Name	Octets	Description
Protocol Identifier	1–2	Protocol being used. The value 0000 0000 0000 0000 identifies the spanning tree algorithm and protocol.
Protocol Version Identifier	3	Identifies the protocol version used.
BPDU Type	4	Value 0000 0000 specifies a configuration BPDU.
CIST Flags	5	Bit 1 is the topology change flag. Bit 2 conveys the CIST proposal flag in RST and MST BPDUs - unused in STP. Bits 3 & 4 convey the CIST port role in RST, and MST BPDUs - unused in STP. Bit 5 conveys the CIST learning flag in RST and MST BPDUs - unused in STP. Bit 6 conveys the CIST forwarding flag in RST and MST BPDUs - unused in STP. Bit 7 conveys the CIST agreement flag in RST and MST BPDUs - unused in STP. Bit 8 conveys the topology change acknowledge flag in STP configuration BPDUs - unused in RSTP and MSTP BPDUs.
CIST Root Identifier	6–13	The Bridge identifier of the CIST Root
CIST External Path Cost	14–17	The path cost between MST regions from the transmitting bridge to the CIST root.
CIST Regional Root Identifier	18–25	ID of the current CIST regional root bridge.
CIST Port Identifier	26–27	CIST port identifier of the transmitting bridge port.
Message Age	28–29	Message age timer value.
Max Age	30–31	Timeout value to be used by all bridges in the bridged network. This value is set by the root. Some implementations of MSTP may choose not to use this value.
Hello Time	32–33	Time interval between the generation of configuration BPDUs by the root bridge.
Forward Delay	34–35	A timeout value used to ensure forward delay timer consistency when transferring a port to the forwarding state. It is also used for ageing filtering database dynamic entries following changes in the active topology.

Table 18-7: MSTP Bridge Protocol Data Units (BPDUs) (cont.)

Field Name	Octets	Description
Version 1 Length	36	Used to convey the Version 1 length. It is always transmitted as 0.
Version 3 Length	37–38	Used to convey the Version 3 length. It is the number of octets taken by the parameters that follow in the BPDU.
MST Configuration Identifier	39–89	An identifier comprising elements of the following: Format Selector Configuration Name Revision Level Configuration Digest.
CIST Internal Root Path Cost	90–93	Path cost to the CIST regional root.
CIST Bridge Identifier	94–101	CIST bridge identifier of the transmitting bridge.
CIST Remaining Hops	102	Remaining hops which limits the propagation and longevity of received spanning tree information for the CIST.
MSTI Configuration Messages (may be absent)	103–39 plus Version 3 Length	See **Table 18-8**.

Table 18-8: MSTI configuration messages

Field Name	Octets	Description
MSTI Flags	1	Bits 1 through 8, convey the topology change flag, proposal flag, port role (two bits), Learning flag, forwarding flag, agreement flag, and master flag for this MSTI.
MSTI Regional Root Identifier	2–9	This includes the value of the MSTID for this configuration message encoded in bits 4 through 1 of octet 1, and bits 8 through 1 of octet 2.
MSTI Internal Root Path Cost	10-13	Internal Root Path Cost.
MSTI Bridge Priority	14	Bits 5 through 8 convey the value of the bridge identifier priority for this MSTI. Bits 1 through 4 of Octet 14 are transmitted as 0, and ignored on receipt.
MSTI Port Priority	15	Bits 5 through 8 are used to convey the value of the port identifier priority for this MSTI. Bits 1 through 4 are transmitted as 0, and ignored on receipt.
MSTI Remaining Hops	16	Value of remaining hops for this MSTI.

Configuring MSTP

By default, RSTP is enabled with default settings on all switch ports. To configure MSTP, see the configuration procedure in **Table 18-9**.

To configure other modes, see **"Configuring RSTP" on page 18.9** or **"Configuring STP" on page 18.6**.

For detailed configuration examples, see the How To Note *How To Configure Basic Switching Functionality*, available from website at **alliedtelesis.com**.

Configuration guidelines for MSTP

- Switches must have the same MST configuration identification elements (region name, revision level and VLAN to MSTI mapping) to be in the same MST region. When configuring multiple MST regions for MSTP, MSTIs are locally significant within an MST region. MSTIs will not span from one region to another region.
- Common and Internal Spanning Tree (CIST) is the default spanning tree instance for MSTP. This means that all VLANs that are not explicitly configured into another MSTI are members of the CIST.
- The software supports a single instance of the MSTP Algorithm consisting of the CIST and up to 15 MSTIs.
- A VLAN can only be mapped to one MSTI or to the CIST. One VLAN mapped to multiple spanning trees is not allowed. All the VLANs are mapped to the CIST by default. Once a VLAN is mapped to a specified MSTI, it is removed from the CIST.
- An MSTI is locally significant within an MST region. An MSTI cannot span across multiple MST regions. The CIST is the spanning tree instance for connecting different MST regions and single spanning tree entities, such as RSTP and STP switches.
- MSTP is compatible with RSTP and STP. An MST region appears as a virtual bridge connecting to single spanning tree entities.
- To avoid unnecessary STP processing, a port that attaches to a LAN that is known to have no other bridges/switches attached can be configured as an edge port.

Before configuring MSTP

Before configuring MSTP, configure VLANs and associate them with switch ports (**Chapter 16, VLAN Introduction** and **Chapter 17, VLAN Commands**), and determine for your network:

- which MSTP regions, revision level and instances are required
- which VLANs and switch ports will belong to which MSTIs,
- which devices you want to be root bridges for each MSTI

Table 18-9: Configuration procedure for MSTP

Command	Description
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `spanning-tree mode mstp`	By default, the device is in RSTP mode. Change to MSTP mode.
`awplus(config)#` `spanning-tree enable`	By default, spanning tree is enabled on all switch ports. If it has been disabled, enable it for MSTP.
Step 1. Configure MSTP region, revision, and instances All MSTP devices in this region of the network must have the same region name, revision number, and VLAN to MSTI mappings.	
`awplus(config)#` spanning-tree mst configuration	Enter MST Configuration mode.
`awplus(config-mst)#` region *<region-name>*	Specify the MSTP region. The **region-name** parameter is an arbitrary string that specifies the name you want to assign to the MST region for identification.
`awplus(config-mst)#` revision *<revision-number>*	The **revision-number** parameter specifies the revision of the current MST configuration. The revision is an arbitrary number that you assign to an MST region. It can be used to keep track of the number of times that MST configuration has been updated for the network. Specify the MST revision number in the range 0 to 255.
`awplus(config-mst)#` instance *<msti-id>* vlan {*<vid>*|*<vid-list>*}	To allow MSTP to block traffic for different VLANs in different places in a loop, create multiple MSTP instances and associate VLANs with them. Each VLAN can only be in one instance. Specify the MST instance ID in the range 1 to 15.

Table 18-9: Configuration procedure for MSTP (cont.)

Command	Description
Step 2. Advanced configuration The commands above are the minimum required to configure MSTP. The following commands allow more advanced configuration.	
Step 3. Assign root bridge priorities MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, and for the CIST, so that each instance blocks a different link. By default, all devices have the same root bridge priority, 32768 (8000 in hexadecimal), so the device with the lowest MAC address becomes the root bridge. If you want the device to be the root bridge for an instance or for the CIST, set the priority to a lower value (a higher priority) than other devices for this instance. (If you enter a number that is not a multiple of 4096, the device rounds the number down.)	
`awplus(config)#` `spanning-tree mst configuration`	Enter MST Configuration mode.
`awplus(config-mst)#` `instance <msti-id> priority <priority>`	Set the priority for the device to become the root bridge for each instance. Specify the MST instance ID in the range 1 to 15. Specify the root bridge priority in the range 0 to 61440. If you enter a number that is not a multiple of 4096, the switch rounds the number down.
`awplus(config-mst)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `spanning-tree priority <priority>`	Set the priority for the device to become the root bridge for the CIST. Specify the bridge priority in the range 0 to 61440. If you enter a number that is not a multiple of 4096, the switch rounds the number down.
Step 4. Configure edge ports If some switch ports are connected to devices that cannot generate BPDUs (such as workstations), you can set particular switch ports as edge ports, or set them to automatically detect whether they are edge ports.	
`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for these switch ports.

`awplus(config-if)#`
`spanning-tree edgeport (RSTP and MSTP)`
or
`awplus(config-if)#`
`spanning-tree autoedge (RSTP and MSTP)`
	Set these ports to be edge ports,
	or
	set these ports to automatically detect whether they are edge ports.

Table 18-9: Configuration procedure for MSTP (cont.)

Command	Description
Step 5. Configure Root Guard	
`awplus(config-if)#` `spanning-tree guard root`	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). Enable the Guard Root feature if required.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
Step 6. Configure BPDU Guard	
`awplus(config)#` `spanning-tree portfast bpdu-guard`	If required, enable the BPDU Guard feature.
`awplus(config)#` `spanning-tree errdisable-timeout enable`	Set a timeout for ports that are disabled due to the BPDU guard feature.
`awplus(config)#` `spanning-tree errdisable-timeout interval <10-1000000>`	Specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.
Step 7. Check MSTP configuration	
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show spanning-tree mst config`	Check that the digest is the same on this device as for all other devices in the same region.
`awplus#` `show spanning-tree mst`	Check the MST to VLAN and port mapping.
`awplus#` `show spanning-tree mst instance <instance>`	Check the detailed information for a particular instance, and all switch ports associated with that instance. Specify the MST instance ID in the range 1 to 15.
`awplus#` `show spanning-tree mst interface <port>`	Check general information about MSTP, and the CIST settings.

Advanced configuration: For most networks, the default settings of the following will be suitable. However, you can also configure them.

- path costs for ports in an MSTI (**spanning-tree mst instance path-cost**) or for the CIST (**spanning-tree path-cost**)
- port priority for ports in an MSTI (**spanning-tree mst instance priority**) or for the CIST (**spanning-tree priority (port priority)**)

Chapter 19: Spanning Tree Commands

Command List 19.3
clear spanning-tree statistics 19.3
clear spanning-tree detected protocols (RSTP and MSTP) 19.4
debug mstp (RSTP and STP) 19.5
instance priority (MSTP) 19.8
instance vlan (MSTP) 19.10
region (MSTP) 19.11
revision (MSTP) 19.12
show debugging mstp 19.13
show spanning-tree 19.14
show spanning-tree brief 19.17
show spanning-tree mst 19.18
show spanning-tree mst config 19.19
show spanning-tree mst detail 19.20
show spanning-tree mst detail interface 19.22
show spanning-tree mst instance 19.24
show spanning-tree mst instance interface 19.25
show spanning-tree mst interface 19.26
show spanning-tree mst detail interface 19.27
show spanning-tree statistics 19.29
show spanning-tree statistics instance 19.30
show spanning-tree statistics instance interface 19.31
show spanning-tree statistics interface 19.32
show spanning-tree vlan range-index 19.34
spanning-tree autoedge (RSTP and MSTP) 19.35
spanning-tree bpdu 19.36
spanning-tree cisco-interoperability (MSTP) 19.38
spanning-tree edgeport (RSTP and MSTP) 19.39
spanning-tree enable 19.40
spanning-tree errdisable-timeout enable 19.42
spanning-tree errdisable-timeout interval 19.43
spanning-tree force-version 19.44
spanning-tree forward-time 19.45
spanning-tree guard root 19.46
spanning-tree hello-time 19.47
spanning-tree link-type 19.48
spanning-tree max-age 19.49
spanning-tree max-hops (MSTP) 19.50
spanning-tree mode 19.51
spanning-tree mst configuration 19.52
spanning-tree mst instance 19.53
spanning-tree mst instance path-cost 19.54
spanning-tree mst instance priority 19.56
spanning-tree mst instance restricted-role 19.57
spanning-tree mst instance restricted-tcn 19.58
spanning-tree path-cost 19.59
spanning-tree portfast (STP) 19.60

spanning-tree portfast bpdu-filter 19.62
spanning-tree portfast bpdu-guard 19.64
spanning-tree priority (bridge priority) 19.66
spanning-tree priority (port priority) 19.67
spanning-tree restricted-role 19.68
spanning-tree restricted-tcn 19.68
spanning-tree transmit-holdcount 19.69
undebug mstp 19.69

Command List

This chapter provides an alphabetical reference for commands used to configure RSTP, STP or MSTP. For information about spanning trees, including configuration procedures, see **Chapter 18, Spanning Tree Introduction: STP, RSTP, and MSTP**

clear spanning-tree statistics

Use this command to clear all the STP BPDU (Bridge Protocol Data Unit) statistics.

Syntax

```
clear spanning-tree statistics

clear spanning-tree statistics [instance <mstp-instance>]

clear spanning-tree statistics
   [interface <port> [instance <mstp-instance>]]
```

Parameter	Description
<port>	The port to clear STP BPDU statistics for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
<mstp-instance>	The MSTP instance (MSTI - Multiple Spanning Tree Instance) to clear MSTP BPDU statistics.

Mode User Exec and Privileged Exec

Usage Use this command with the **instance** parameter in MSTP mode. Specifying this command with the **interface** parameter only not the instance parameter will work in STP and RSTP mode.

Examples

```
awplus# clear spanning-tree statistics

awplus# clear spanning-tree statistics instance 1

awplus# clear spanning-tree statistics interface port1.0.2

awplus# clear spanning-tree statistics interface port1.0.2
       instance 1
```

clear spanning-tree detected protocols (RSTP and MSTP)

Use this command to clear the detected protocols for a specific port, or all ports.

Use this command in RSTP or MSTP mode only.

Syntax `clear spanning-tree detected protocols [interface <port>]`

Parameter	Description
<port>	The port to clear detected protocols for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example

```
awplus# clear spanning-tree detected protocols
```

debug mstp (RSTP and STP)

Use this command to enable debugging for the configured spanning tree mode, and echo data to the console, at various levels. Note that although this command uses the keyword **mstp** it displays debugging output for RSTP and STP protocols as well the MSTP protocol.

Use the **no** variant of this command to disable spanning tree debugging.

Syntax

```
debug mstp {all|cli|protocol [detail]|timer [detail]}
debug mstp {packet {rx|tx} [decode] [interface <interface>]}
debug mstp {topology-change [interface <interface>]}
no debug mstp {all|cli|protocol [detail]|timer [detail]}
no debug mstp {packet {rx|tx} [decode] [interface <interface>]}
no debug mstp {topology-change [interface <interface>]}
```

Parameter	Description
`all`	Echoes all spanning tree debugging levels to the console.
`cli`	Echoes spanning tree commands to the console.
`packet`	Echoes spanning tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`timer`	Echoes timer information to the console.
`detail`	Detailed output.
`decode`	Interprets packet contents
`topology-change`	Interprets topology change messages
`interface`	Keyword before <*interface*> placeholder to specify an interface to debug
<*interface*>	Placeholder used to specify the name of the interface to debug.

Mode Privileged Exec and Global Configuration mode

Usage 1 Use the **debug mstp topology-change interface** command to generate debugging messages when the switch receives an indication of a topology change in a BPDU from another device. The debugging can be activated on a per-port basis. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the **terminal monitor** command on page 8.69 before issuing the relevant **debug mstp** command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using **log buffered (filter)** command on page 10.8:

```
awplus# configure terminal
awplus(config)# log buffered program mstp
```

Output 1

```
awplus#terminal monitor
awplus#debug mstp topology-change interface port1.0.4
10:09:09 awplus MSTP[1409]: Topology change rcvd on port1.0.4 (internal)
10:09:09 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.4
aawplus#debug mstp topology-change interface port1.0.6
10:09:29 awplus MSTP[1409]: Topology change rcvd on port1.0.6 (external)
10:09:29 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.6
```

Usage 2 Use the **debug mstp packet rx|tx decode interface** command to generate debugging messages containing the entire contents of a BPDU displayed in readable text for transmitted and received xSTP BPDUs. The debugging can be activated on a per-port basis and transmit and receive debugging is controlled independently. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the **terminal monitor** command on page 8.69 before issuing the relevant **debug mstp** command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using the **log buffered (filter)** command on page 10.8:

```
awplus(config)# log buffered program mstp
```

Output 2 In MSTP mode - an MSTP BPDU with 1 MSTI:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:23:42 awplus MSTP[1417]: Protocol version: MSTP, BPDU type: RST
17:23:42 awplus MSTP[1417]: CIST Flags:  Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: CIST root id      : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST ext pathcost : 0
17:23:42 awplus MSTP[1417]: CIST reg root id  : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:23:42 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:23:42 awplus MSTP[1417]: Version 3 length : 80
17:23:42 awplus MSTP[1417]: Format id      : 0
17:23:42 awplus MSTP[1417]: Config name    : test
17:23:42 awplus MSTP[1417]: Revision level : 0
17:23:42 awplus MSTP[1417]: Config digest  : 3ab68794d602fdf43b21c0b37ac3bca8
17:23:42 awplus MSTP[1417]: CIST int pathcost : 0
17:23:42 awplus MSTP[1417]: CIST bridge id    : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST hops remaining : 20
17:23:42 awplus MSTP[1417]: MSTI flags           : Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: MSTI reg root id     : 8001:0000cd1000fe
17:23:42 awplus MSTP[1417]: MSTI pathcost        : 0
17:23:42 awplus MSTP[1417]: MSTI bridge priority : 32768 port priority : 128
17:23:42 awplus MSTP[1417]: MSTI hops remaining  : 20
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In STP mode transmitting a TCN BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet tx decode interface port1.0.4
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - start
17:28:09 awplus MSTP[1417]: Protocol version: STP, BPDU type: TCN
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - finish
```

In STP mode receiving an STP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:31:36 awplus MSTP[1417]: Protocol version: STP, BPDU type: Config
17:31:36 awplus MSTP[1417]: Flags:  role=none
17:31:36 awplus MSTP[1417]: Root id      : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Root pathcost : 0
17:31:36 awplus MSTP[1417]: Bridge id  : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Port id      : 8001 (128:1)
17:31:36 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:31:36 awplus MSTP[1417]: ort1.0.4 xSTP BPDU rx - finish
```

In RSTP mode receiving an RSTP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
awplus#17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:30:17 awplus MSTP[1417]: Protocol version: RSTP, BPDU type: RST
17:30:17 awplus MSTP[1417]: CIST Flags:  Forward Learn role=Desig
17:30:17 awplus MSTP[1417]: CIST root id      : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST ext pathcost : 0
17:30:17 awplus MSTP[1417]: CIST reg root id  : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:30:17 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

Examples

```
awplus# debug mstp all

awplus# debug mstp cli

awplus# debug mstp packet rx

awplus# debug mstp protocol detail

awplus# debug mstp timer

awplus# debug mstp packet rx decode interface port1.0.2

awplus# debug mstp packet tx decode interface port1.0.6
```

Related Commands

log buffered (filter)
show debugging mstp
terminal monitor
undebug mstp

instance priority (MSTP)

Use this command to set the priority for this device to become the root bridge for the specified MSTI (Multiple Spanning Tree Instance).

Use this command for MSTP only.

Use the **no** variant of this command to restore the root bridge priority of the device for the instance to the default.

Syntax

```
instance <msti-id> priority <priority>
no instance <msti-id> priority
```

Parameter	Description
<msti-id>	Specify the The MST instance ID in the range <1-15>.
<priority>	Specify the root bridge priority for the device for the MSTI in the range <0-61440>. Note that a lower priority number indicates a greater likelihood of the device becoming the root bridge. The priority values can be set only in increments of 4096. If you specify a number that is not a multiple of 4096, it will be rounded down. The default priority is 32768.

Default The default priority value for all instances is 32768.

Mode MST Configuration

Usage MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, so that each instance blocks a different link.
If all devices have the same root bridge priority for the instance, MSTP selects the device with the lowest MAC address to be the root bridge. Give the device a higher priority for becoming the root bridge for a particular instance by assigning it a lower priority number, or vice versa.

Examples To set the root bridge priority for MSTP instance 2 to be the highest (0), so that it will be the root bridge for this instance when available, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 priority 0
```

To reset the root bridge priority for instance 2 to the default (32768), use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 2 priority
```

Related Commands

region (MSTP)
revision (MSTP)
show spanning-tree mst config
spanning-tree mst instance
spanning-tree mst instance priority

instance vlan (MSTP)

Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR). An MSTR can contain up to 15 MSTIs.

When a VLAN is associated with an MSTI the member ports of the VLAN are automatically configured to send and receive spanning-tree information for the associated MSTI. You can disable this automatic configuration of member ports of the VLAN to the associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI.

Use the **instance vlan** command for MSTP only.

Use the **no** variant of this command to remove the specified VLANs from the MSTI.

Syntax

```
instance <msti-id> vlan {<vid>|<vid-list>}
no instance <msti-id> vlan {<vid>|<vid-list>}
```

Parameter	Description
<msti-id>	Specify the MST instance ID <1-15>.
<vid>	Specify a VLAN identifier (VID) in the range <1-4094> to be associated with the MSTI specified.
<vid-list>	A hyphen-separated range or a comma-separated list of VLAN IDs

Mode MST Configuration

Usage The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

This command removes the specified VLANs from the CIST and adds them to the specified MSTI. If you use the **no** variant of this command to remove the VLAN from the MSTI, it returns it to the CIST. To move a VLAN from one MSTI to another, you must first use the **no** variant of this command to return it to the CIST.

Ports in these VLANs will remain in the control of the CIST until you associate the ports with the MSTI using the **spanning-tree mst instance** command.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 vlan 30
```

Related Commands

region (MSTP)
revision (MSTP)
show spanning-tree mst config
spanning-tree mst instance
vlan

region (MSTP)

Use this command to assign a name to the device's MST Region. MST Instances (MSTI) of a region form different spanning trees for different VLANs.

Use this command for MSTP only.

Use the **no** variant of this command to remove this region name and reset it to the default.

Syntax

```
region <region-name>
no region
```

Parameter	Description
<region-name>	Specify the name of the region, up to 32 characters. Valid characters are upper-case, lower-case, digits, underscore.

Default By default, the region name is My Name.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# region ATL
```

Related Commands **revision (MSTP)**
show spanning-tree mst config

revision (MSTP)

Use this command to specify the MST revision number to be used in the configuration identifier.

Use this command for MSTP only.

Syntax `revision <revision-number>`

Parameter	Description
<revision-number>	<0-65535> Revision number.

Default The default of revision number is 0.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 25
```

Related Commands **region (MSTP)**
show spanning-tree mst config
instance vlan (MSTP)

show debugging mstp

Use this command to show the MSTP debugging options set.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging mstp`

Mode User Exec and Privileged Exec mode

Example To display the MSTP debugging options set, enter the command:

```
awplus# show debugging mstp
```

Output **Figure 19-1: Example output from the show debugging mstp command**

```
MSTP debugging status:
  MSTP receiving packet debugging is on
```

Related Commands **debug mstp (RSTP and STP)**

show spanning-tree

Use this command to display detailed spanning tree information on the specified port or on all ports. Use this command for RSTP, MSTP or STP.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree [interface <port-list>]`

Parameter	Description
`interface`	Display information about the following port only.
`<port-list>`	The ports to display information about. A port-list can be: ■ a switch port (e.g. `port1.0.6`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Mode User Exec and Privileged Exec

Usage Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display spanning tree information about `port1.0.3`, use the command:

```
awplus# show spanning-tree interface port1.0.3
```

Output **Figure 19-2: Example output from the show spanning-tree command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd20f093
% 1: Bridge Id 80000000cd20f093
% 1: last topology change Sun Nov 20 12:24:24 1977
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.3: Port 5023 - Id 839f - Role Designated - State Forwarding
%   port1.0.3: Designated Path Cost 0
%   port1.0.3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 839f - Priority 128  -
%   port1.0.3: Root 80000000cd20f093
%   port1.0.3: Designated Bridge 80000000cd20f093
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: Hello Time 2 - Forward Delay 15
%   port1.0.3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.0.3: forward-transitions 32
%   port1.0.3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current point-to-point
.
.
```

Figure 19-3: Example output from the show spanning-tree command in RSTP mode

```
awplus#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd24ff2d
% 1: Bridge Id 80000000cd24ff2d
% 1: last topology change Thu Jul 26 02:06:26 2007
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - Priority 128  -
%   port1.0.1: Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.1: forward-transitions 0
%   port1.0.1: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.1: No portfast configured - Current  portfast off
%   port1.0.1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.1: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.1: no root guard configured     - Current root guard off
%   port1.0.1: Configured Link Type point-to-point - Current  shared
%
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.2: Designated Port Id 838a - Priority 128  -
%   port1.0.2: Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
```

show spanning-tree brief

Use this command to display a summary of spanning tree status information on all ports. Use this command for RSTP, MSTP or STP.

Syntax `show spanning-tree brief`

Parameter	Description
`brief`	A brief summary of spanning tree information.

Mode User Exec and Privileged Exec

Usage Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display a summary of spanning tree status information, use the command:

```
awplus# show spanning-tree brief
```

Output **Figure 19-4: Example output from the show spanning-tree brief command**

```
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 40000 - Root Port 4501 -  Bridge Priority 32768
Default: Root Id 8000:0000cd250001
Default: Bridge Id 8000:0000cd296eb1

Port            Designated Bridge    Port Id    Role          State
sa1             8000:001577c9744b    8195       Rootport      Forwarding
po1             8000:0000cd296eb1    81f9       Designated    Forwarding
port1.0.1       8000:0000cd296eb1    8389       Disabled      Discarding
port1.0.2       8000:0000cd296eb1    838a       Disabled      Discarding
port1.0.3       8000:0000cd296eb1    838b       Disabled      Discarding
port1.0.4       8000:0000cd296eb1    838c       Disabled      Discarding
port1.0.5       8000:0000cd296eb1    838d       Disabled      Discarding
port1.0.6       8000:0000cd296eb1    838e       Disabled      Discarding
```

Related Commands **show spanning-tree**

show spanning-tree mst

This command displays bridge-level information about the CIST and VLAN to MSTI mappings.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst`

Mode User Exec, Privileged Exec and Interface Configuration

Example To display bridge-level information about the CIST and VLAN to MSTI mappings, enter the command:

```
awplus# show spanning-tree mst
```

Output **Figure 19-5: Example output from the show spanning-tree mst command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000475e93ffe
% 1: CIST Reg Root Id 8000000475e93ffe
% 1: CST Bridge Id 8000000475e93ffe
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%
%   Instance        VLAN
%   0:              1
%   2:              4
```

Related Commands **show spanning-tree mst interface**

show spanning-tree mst config

Use this command to display MSTP configuration identifier for the device.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst config`

Mode User Exec, Privileged Exec and Interface Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example To display MSTP configuration identifier information, enter the command:

```
awplus# show spanning-tree mst config
```

Output **Figure 19-6: Example output from the show spanning-tree mst config command**

```
awplus#show spanning-tree mst config
%
%  MSTP Configuration Information:
%-----------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0x80DEE46DA92A98CF21C603291B22880A
%-----------------------------------------------------
```

Related Commands
instance vlan (MSTP)
region (MSTP)
revision (MSTP)

show spanning-tree mst detail

This command displays detailed information about each instance, and all interfaces associated with that particular instance.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst detail`

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, enter the command:

```
awplus# show spanning-tree mst detail
```

Output **Figure 19-7: Example output from the show spanning-tree mst detail command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - CIST Priority 128  -
%   port1.0.1: CIST Root 80000000cd24ff2d
%   port1.0.1: Regional Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: CIST Hello Time 2 - Forward Delay 15
%   port1.0.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
.
.
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
%   port1.0.3: Port 5003 - Id 838b - Role Disabled - State Discarding
%   port1.0.3: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.3: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 838b - CIST Priority 128  -
%   port1.0.3: CIST Root 80000000cd24ff2d
%   port1.0.3: Regional Root 80000000cd24ff2d
%   port1.0.3: Designated Bridge 80000000cd24ff2d
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: CIST Hello Time 2 - Forward Delay 15
%   port1.0.3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.3: forward-transitions 0
%   port1.0.3: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current  shared
```

show spanning-tree mst detail interface

This command prints detailed information about the specified switch port, and the MST instances associated with it.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst detail interface <port>`

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about `port1.0.3` and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

Output **Figure 19-8: Example output from the show spanning-tree mst detail interface command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   port1.0.2: Designated Port Id 838a - CIST Priority 128  -
%   port1.0.2: CIST Root 80000000cd24ff2d
%   port1.0.2: Regional Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: CIST Hello Time 2 - Forward Delay 15
%   port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
% Instance  2:  Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

show spanning-tree mst instance

This command displays detailed information for the specified instance, and all switch ports associated with that instance.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst instance <instance>`

Parameter	Description
<instance>	Specify an MSTP instance in the range <1-15>.

Mode User Exec, Privileged Exec, and Interface Configuration

Usage To display detailed information for **instance 2**, and all switch ports associated with that instance, use the command:

```
awplus# show spanning-tree mst instance 2
```

Output **Figure 19-9: Example output from the show spanning-tree mst instance command**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst instance interface

This command displays detailed information for the specified MST (Multiple Spanning Tree) instance, and the specified switch port associated with that MST instance.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst instance <instance> interface <port>`

Parameter	Description
<instance>	Specify an MSTP instance in the range `<1-15>`.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information for `instance 2`, interface `port1.0.2`, use the command:

```
awplus# show spanning-tree mst instance 2 interface port1.0.2
```

Output **Figure 19-10: Example output from the show spanning-tree mst instance command**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst interface

This command displays the number of instances created, and VLANs associated with it for the specified switch port.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst interface <port>`

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, for `port1.0.4`, use the command:

```
awplus# show spanning-tree mst interface port1.0.4
```

Output **Figure 19-11: Example output from the show spanning-tree mst interface command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
%   Instance        VLAN
%   0:              1
%   1:              2-3
%   2:              4-5
```

show spanning-tree mst detail interface

This command displays detailed information about the specified switch port, and the MST instances associated with it.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree mst detail interface <port>`

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about `port1.0.3` and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

Output **Figure 19-12: Example output from the show spanning-tree mst detail interface command**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   port1.0.2: Designated Port Id 838a - CIST Priority 128  -
%   port1.0.2: CIST Root 80000000cd24ff2d
%   port1.0.2: Regional Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: CIST Hello Time 2 - Forward Delay 15
%   port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
% Instance  2:  Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

show spanning-tree statistics

This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances. For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree statistics`

Mode Privileged Exec

Usage To display BPDU statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances, use the command:

```
awplus# show spanning-tree statistics
```

Output **Figure 19-13: Example output from the show spanning-tree statistics command**

```
Port number = 915 Interface = port1.0.6
                ================================
% BPDU Related Parameters
% ------------------------
% Port Spanning Tree                 : Disable
% Spanning Tree Type                 : Rapid Spanning Tree Protocol
% Current Port State                 : Discarding
% Port ID                            : 8393
% Port Number                        : 393
% Path Cost                          : 20000000
% Message Age                        : 0
% Designated Root                    : ec:cd:6d:20:c0:ed
% Designated Cost                    : 0
% Designated Bridge                  : ec:cd:6d:20:c0:ed
% Designated Port Id                 : 8393
% Top Change Ack                     : FALSE
% Config Pending                     : FALSE
% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted              : 0
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 0
% TCN Bpdu's received                : 0
% Forward Trans Count                : 0
% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : INACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0
% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 0
% Next State                         : Learning
% Topology Change Time               : 0
```

show spanning-tree statistics instance

This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance, and all switch ports associated with that MST instance. For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree statistics instance <instance>`

Parameter	Description
<instance>	Specify an MSTP instance in the range <1-15>.

Mode Privileged Exec

Usage To display BPDU statistics information for MST instance 2, and all switch ports associated with that MST instance, use the command:

```
awplus# show spanning-tree statistics instance 2
```

Output **Figure 19-14: Example output from the show spanning-tree statistics instance command:**

```
% % INST_PORT port1.0.3 Information & Statistics
% ----------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.3: Forward Transitions                  : 0
% Next State                           : Learning
% Topology Change Time                 : 0
% INST_PORT port1.0.4 Information & Statistics
% ----------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.4: Forward Transitions                  : 0
% Next State                           : Learning
% Topology Change Time                 : 0
% INST_PORT port1.0.5 Information & Statistics
% ----------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.5: Forward Transitions                  : 0
% Next State                           : Learning
% Topology Change Time                 : 0%
```

Related Commands **show spanning-tree statistics**

show spanning-tree statistics instance interface

This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree statistics instance <instance> interface <port>`

Parameter	Description
<instance>	Specify an MSTP instance in the range `<1-15>`.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example To display BPDU statistics for MST `instance 2`, interface `port1.0.2`, use the command:

```
awplus# show spanning-tree statistics instance 2 interface
       port1.0.2
```

Output **Figure 19-15: Example output from the show spanning-tree statistics instance interface command**

```
awplus#sh spanning-tree statistics interface port1.0.2 instance 1
        Spanning Tree Enabled for Instance : 1
        ================================
% INST_PORT port1.0.2 Information & Statistics
% ------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.2: Forward Transitions                 : 0
% Next State                           : Learning
% Topology Change Time                 : 0

% Other Inst/Vlan Information & Statistics
% ------------------------------------
% Bridge Priority                    : 0
% Bridge Mac Address                 : ec:cd:6d:20:c0:ed
% Topology Change Initiator          : 5023
% Last Topology Change Occured       : Mon Aug 22 05:42:06 2011
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 1
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Related Commands **show spanning-tree statistics**

show spanning-tree statistics interface

This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree statistics interface <port>`

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example To display BPDU statistics about each MST instance for `port1.0.4`, use the command:

```
awplus# show spanning-tree statistics interface port1.0.4
```

Output **Figure 19-16: Example output from the show spanning-tree statistics interface command**

```
awplus#show spanning-tree statistics interface port1.0.2

                Port number = 906 Interface = port1.0.2
                ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Disable
% Spanning Tree Type                : Multiple Spanning Tree Protocol
% Current Port State                : Discarding
% Port ID                           : 838a
% Port Number                       : 38a
% Path Cost                         : 20000000
% Message Age                       : 0
% Designated Root                   : ec:cd:6d:20:c0:ed
% Designated Cost                   : 0
% Designated Bridge                 : ec:cd:6d:20:c0:ed
% Designated Port Id                : 838a
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted             : 0
% Config Bpdu's received            : 0
% TCN Bpdu's xmitted                : 0
% TCN Bpdu's received               : 0
% Forward Trans Count               : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured             : 2
% Hello timer                       : INACTIVE
% Hello Time Value                  : 0
% Forward Delay Timer               : INACTIVE
% Forward Delay Timer Value         : 0
% Message Age Timer                 : INACTIVE
% Message Age Timer Value           : 0
% Topology Change Timer             : INACTIVE
% Topology Change Timer Value       : 0
% Hold Timer                        : INACTIVE
% Hold Timer Value                  : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions               : 1
% Msg Age Expiry                    : 0
% Similar BPDUS Rcvd                : 0
% Src Mac Count                     : 0
% Total Src Mac Rcvd                : 0
% Next State                        : Learning
% Topology Change Time              : 0


% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address             : 01:80:c2:00:00:00
% Bridge Priority                   : 32768
% Bridge Mac Address                : ec:cd:6d:20:c0:ed
% Bridge Hello Time                 : 2
% Bridge Forward Delay              : 15
% Topology Change Initiator         : 5023
% Last Topology Change Occured      : Mon Aug 22 05:41:20 2011
% Topology Change                   : FALSE
% Topology Change Detected          : TRUE
% Topology Change Count             : 1
% Topology Change Last Recvd from   : 00:00:00:00:00:00
```

Related Commands **show spanning-tree statistics**

show spanning-tree vlan range-index

Use this command to display information about MST (Multiple Spanning Tree) instances and the VLANs associated with them including the VLAN range-index value for the switch.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show spanning-tree vlan range-index`

Mode Privileged Exec

Example To display information about MST instances and the VLANs associated with them for the switch, including the VLAN range-index value, use the following command:

```
awplus# show spanning-tree vlan range-index
```

Output **Figure 19-17: Example output from the show spanning-tree vlan range-index command**

```
awplus#show spanning-tree vlan range-index
% MST Instance  VLAN       RangeIdx
%      1        1          1
%
```

Related Commands **show spanning-tree statistics**

spanning-tree autoedge (RSTP and MSTP)

Use this command to enable the autoedge feature on the port.

The autoedge feature allows the port to automatically detect that it is an edge port. If it does not receive any BPDUs in the first three seconds after linkup, enabling, or entering RSTP or MSTP mode, it sets itself to be an edgeport and enters the forwarding state.

Use this command for RSTP or MSTP.

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

Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default Disabled

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# spanning-tree autoedge
```

Related Commands spanning-tree edgeport (RSTP and MSTP)

spanning-tree bpdu

Use this command in Global Configuration mode to configure BPDU (Bridge Protocol Data Unit) discarding or forwarding, with STP (Spanning Tree Protocol) disabled on the switch.

See the **Usage** note about disabling Spanning Tree before using this command, and using this command to forward unsupported BPDUs unchanged for unsupported STP Protocols.

There is not a **no** variant for this command. Instead, apply the `discard` parameter to reset it back to the default then re-enable STP with **spanning-tree enable** command.

Syntax

```
spanning-tree bpdu {discard|forward|forward-untagged-vlan|
    forward-vlan}
```

Parameter	Description	
`bpdu`	A port that has BPDU filtering enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Global Configuration mode):	
	`discard`	Discards all ingress STP BPDU frames.
	`forward`	Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership.
	`forward-untagged-vlan`	Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN.
	`forward-vlan`	Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN.

Default The discard parameter is enabled by default.

Mode Global Configuration

Usage You must first disable Spanning Tree with the **no spanning-tree {mstp|rstp|stp} enable** command before you can use this command to then configure BPDU discarding or forwarding.

This command enables the switch to forward unsupported BPDUs with an unsupported Spanning Tree Protocol, such as proprietary STP protocols with unsupported BPDUs, by forwarding BDPU (Bridge Protocol Data Unit) frames unchanged through the switch.

When you want to revert to default behavior on the switch, issue a **spanning-tree bdpu discard** command and re-enable Spanning Tree with a **spanning-tree enable** command.

Examples To enable STP BPDU discard in Global Configuration mode with STP disabled, which discards all ingress STP BPDU frames, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu discard
```

To enable STP BPDU forward in Global Configuration mode with STP disabled, which

forwards any ingress STP BPDU frames to all ports regardless of any VLAN membership, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward
```

To enable STP BPDU forwarding for untagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-untagged-vlan
```

To enable STP BPDU forwarding for tagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-vlan
```

To reset STP BPDU back to the default `discard` parameter and re-enable STP on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree bpdu discard
awplus(config)# spanning-tree stp enable
```

Related Commands **show spanning-tree**
spanning-tree enable

spanning-tree cisco-interoperability (MSTP)

Use this command to enable/disable Cisco-interoperability for MSTP.

Use this command for MSTP only.

Syntax `spanning-tree cisco-interoperability {enable|disable}`

Parameter	Description
`enable`	Enable Cisco interoperability for MSTP.
`disable`	Disable Cisco interoperability for MSTP.

Default If this command is not used, Cisco interoperability is disabled.

Mode Global Configuration

Usage For compatibility with certain Cisco devices, all devices in the switched LAN running the AlliedWare Plus™ Operating System must have Cisco-interoperability enabled. When the AlliedWare Plus™ Operating System is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

Examples To enable Cisco interoperability on a Layer 2 switch:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 switch:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability disable
```

spanning-tree edgeport (RSTP and MSTP)

Use this command to set a port as an edge-port.

Use this command for RSTP or MSTP.

This command has the same effect as the **spanning-tree portfast (STP)** command, but the configuration displays differently in the output of some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default Not an edge port.

Mode Interface Configuration

Usage Use this command on a switch port connected to a LAN that has no other bridges attached. If a BPDU is received on the port that indicates that another bridge is connected to the LAN, then the port is no longer treated as an edge port.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree edgeport
```

Related Commands **spanning-tree autoedge (RSTP and MSTP)**

spanning-tree enable

Use this command in Global Configuration mode to enable the specified spanning tree protocol for all switch ports. Note that this must be the spanning tree protocol that is configured on the switch by the **spanning-tree mode** command.

Use the **no** variant of this command to disable the configured spanning tree protocol. This places all switch ports in the forwarding state.

Syntax

```
spanning-tree {mstp|rstp|stp} enable
no spanning-tree {mstp|rstp|stp} enable
```

Parameter	Description
`mstp`	Enables or disables MSTP (Multiple Spanning Tree Protocol).
`rstp`	Enables or disables RSTP (Rapid Spanning Tree Protocol).
`stp`	Enables or disables STP (Spanning Tree Protocol).

Default RSTP is enabled by default for all switch ports.

Mode Global Configuration

Usage With no configuration, spanning tree is enabled, and the spanning tree mode is set to RSTP. To change the mode, see **spanning-tree mode** command on page 19.51.

Examples To enable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

To disable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

To enable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

To disable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable
```

To enable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

To disable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

Related Commands **spanning-tree bpdu**
spanning-tree mode

spanning-tree errdisable-timeout enable

Use this command to enable the errdisable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable the errdisable-timeout facility.

Syntax

```
spanning-tree errdisable-timeout enable
no spanning-tree errdisable-timeout enable
```

Default By default, the errdisable-timeout is disabled.

Mode Global Configuration

Usage The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port is re-enabled without manual intervention after a set interval. This interval can be configured by the user using the **spanning-tree errdisable-timeout interval** command.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
```

Related Commands

show spanning-tree
spanning-tree errdisable-timeout interval
spanning-tree portfast bpdu-guard

spanning-tree errdisable-timeout interval

Use this command to specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.

Use this command for RSTP or MSTP.

Syntax

```
spanning-tree errdisable-timeout interval <10-1000000>
no spanning-tree errdisable-timeout interval
```

Parameter	Description
<10-1000000>	Specify the errdisable-timeout interval in seconds.

Default By default, the port is re-enabled after 300 seconds.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval 34
```

Related Commands

show spanning-tree
spanning-tree errdisable-timeout enable
spanning-tree portfast bpdu-guard

spanning-tree force-version

Use this command in Interface Configuration mode for a switch port interface only to force the protocol version for the switch port. Use this command for RSTP or MSTP only.

Syntax

```
spanning-tree force-version <version>
no spanning-tree force-version
```

Parameter	Description	
<version>	<0-3>	Version identifier.
	0	Forces the port to operate in STP mode.
	1	Not supported.
	2	Forces the port to operate in RSTP mode. If it receives STP BPDUs, it can automatically revert to STP mode.
	3	Forces the port to operate in MSTP mode (this option is only available if MSTP mode is configured). If it receives RSTP or STP BPDUs, it can automatically revert to RSTP or STP mode.

Default By default, no version is forced for the port. The port is in the spanning tree mode configured for the device, or a lower version if it automatically detects one.

Mode Interface Configuration mode for a switch port interface only.

Examples Set the value to enforce the spanning tree protocol (STP):

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree force-version 0
```

Set the default protocol version:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree force-version
```

Related Commands show spanning-tree

spanning-tree forward-time

Use this command to set the forward delay value. Use the **no** variant of this command to reset the forward delay value to the default setting of 15 seconds.

The **forward delay** sets the time (in seconds) to control how fast a port changes its spanning tree state when moving towards the forwarding state. If the mode is set to STP, the value determines how long the port stays in each of the listening and learning states which precede the forwarding state. If the mode is set to RSTP or MSTP, this value determines the maximum time taken to transition from discarding to learning and from learning to forwarding.

This value is used only when the switch is acting as the root bridge. Switches not acting as the Root Bridge use a dynamic value for the **forward delay** set by the root bridge. The **forward delay**, **max-age**, and **hello time** parameters are interrelated.

Syntax

```
spanning-tree forward-time <forward-delay>
no spanning-tree forward-time
```

Parameter	Description
<forward-delay	<4-30> The forwarding time delay in seconds.

Default The default is 15 seconds.

Mode Global Configuration

Usage The allowable range for forward-time is 4-30 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree forward-time 6
```

Related Commands

show spanning-tree
spanning-tree forward-time *<forward-delay>*
spanning-tree hello-time *<hello-time>*
spanning-tree mode

spanning-tree guard root

Use this command in Interface Configuration mode for a switch port only to enable the Root Guard feature for the switch port. The root guard feature disables reception of superior BPDUs. You can use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to disable the root guard feature for the port.

Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Mode Interface Configuration mode for a switch port interface only.

Usage The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree guard root
```

spanning-tree hello-time

Use this command to set the hello-time. This sets the time in seconds between the transmission of switch spanning tree configuration information when the switch is the Root Bridge of the spanning tree or is trying to become the Root Bridge.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of the hello time.

Syntax

```
spanning-tree hello-time <hello-time>
no spanning-tree hello-time
```

Parameter	Description
<hello-time>	<1-10> The hello BPDU interval in seconds.

Default Default is 2 seconds.

Mode Global Configuration and Interface Configuration for switch ports.

Usage The allowable range of values is 1-10 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (**forward delay** - 1.0 seconds) >= **max-age**

max-age >= 2 x (**hello time** + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree hello-time 3
```

Related Commands

spanning-tree forward-time *<forward-delay>*
spanning-tree max-age *<max-age>*
show spanning-tree

spanning-tree link-type

Use this command in Interface Configuration mode for a switch port interface only to enable or disable point-to-point or shared link types on the switch port.

Use this command for RSTP or MSTP only.

Use the **no** variant of this command to return the port to the default link type.

Syntax

```
spanning-tree link-type {point-to-point|shared}
no spanning-tree link-type
```

Parameter	Description
`shared`	Disable rapid transition.
`point-to-point`	Enable rapid transition.

Default The default link type is point-to-point.

Mode Interface Configuration mode for a switch port interface only.

Usage You may want to set link type to shared if the port is connected to a hub with multiple switches connected to it.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# spanning-tree link-type point-to-point
```

spanning-tree max-age

Use this command to set the max-age. This sets the maximum age, in seconds, that dynamic spanning tree configuration information is stored in the switch before it is discarded.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of max-age.

Syntax

```
spanning-tree max-age <max-age>
no spanning-tree max-age
```

Parameter	Description
<max-age>	<6-40> The maximum time, in seconds.

Default The default of spanning-tree max-age is 20 seconds.

Mode Global Configuration

Usage Max-age is the maximum time in seconds for which a message is considered valid.

Configure this value sufficiently high, so that a frame generated by the root bridge can be propagated to the leaf nodes without exceeding the max-age.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree max-age 12
```

Related Commands

show spanning-tree
spanning-tree forward-time *<forward-delay>*
spanning-tree hello-time *<hello-time>*

spanning-tree max-hops (MSTP)

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST region.

Use the **no** variant of this command to restore the default.

Use this command for MSTP only.

Syntax

```
spanning-tree max-hops <hop-count>
no spanning-tree max-hops <hop-count>
```

Parameter	Description
<hop-count>	Specify the maximum hops the BPDU will be valid for in the range <1-40>.

Default The default max-hops in a MST region is 20.

Mode Global Configuration

Usage Specifying the max hops for a BPDU prevents the messages from looping indefinitely in the network. The hop count is decremented by each receiving port. When a switch receives an MST BPDU that has a hop count of zero, it discards the BPDU.

Examples

```
awplus# configure terminal
awplus(config)# spanning-tree max-hops 25

awplus# configure terminal
awplus(config)# no spanning-tree max-hops
```

spanning-tree mode

Use this command to change the spanning tree protocol mode on the switch. The spanning tree protocol mode on the switch can be configured to either STP, RSTP or MSTP.

Syntax `spanning-tree mode {stp|rstp|mstp}`

Default The default spanning tree protocol mode on the switch is RSTP.

Mode Global Configuration

Usage With no configuration, the switch will have spanning tree enabled, and the spanning tree mode will be set to RSTP. Use this command to change the spanning tree protocol mode on the device. MSTP is VLAN aware, but RSTP and STP are not VLAN aware. To enable or disable spanning tree operation, see the **spanning-tree enable** command on page 19.40.

Examples To change the spanning tree mode from the default of RSTP to MSTP, use the following commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

Related Commands **spanning-tree enable**

spanning-tree mst configuration

Use this command to enter the MST Configuration mode to configure the Multiple Spanning-Tree Protocol.

Syntax `spanning-tree mst configuration`

Mode Global Configuration

Examples The following example uses this command to enter MST Configuration mode. Note the change in the command prompt.

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```

spanning-tree mst instance

Use this command in Interface Configuration mode to assign a Multiple Spanning Tree instance (MSTI) to a switch port or channel group.

Note that ports are automatically configured to send and receive spanning-tree information for the associated MSTI when VLANs are assigned to MSTIs using the **instance vlan (MSTP)** command.

Use the **no** variant of this command in Interface Configuration mode to remove the MSTI from the specified switch port or channel group.

Syntax

```
spanning-tree mst instance <instance-id>
no spanning-tree mst instance <instance-id>
```

Parameter	Description
<instance-id>	<1-15> Specify the MST instance ID. The MST instance must have already been created using the **instance vlan (MSTP)** command.

Default A port automatically becomes a member of an MSTI when it is assigned to a VLAN.

Mode Interface Configuration mode for a switch port or channel group.

Usage You can disable automatic configuration of member ports of a VLAN to an associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI. Use the **spanning-tree mst instance** command to add a VLAN member port back to the MSTI.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
```

Related Commands

instance vlan (MSTP)
spanning-tree mst instance path-cost
spanning-tree mst instance priority
spanning-tree mst instance restricted-role
spanning-tree mst instance restricted-tcn

spanning-tree mst instance path-cost

Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path associated with a switch port, for the specified MSTI (Multiple Spanning Tree Instance) identifier.

This specifies the switch port's contribution to the cost of a path to the MSTI regional root via that port. This applies when the port is the root port for the MSTI.

Use the **no** variant of this command to restore the default cost value of the path.

Syntax

```
spanning-tree mst instance <instance-id> path-cost <path-cost>
no spanning-tree mst instance <instance-id> path-cost
```

Parameter	Description
<instance-id>	Specify the MSTI identifier in the range <1-15>.
<path-cost>	Specify the cost of path in the range of <1-200000000>, where a lower path-cost indicates a greater likelihood of the specific interface becoming a root.

Default

The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 standard.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2, 000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode

Interface Configuration mode for a switch port interface only.

Usage

Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the `spanning-tree instance` command.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 path-cost 1000
```

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 path-cost
```

Related Commands

instance vlan (MSTP)
spanning-tree mst instance
spanning-tree mst instance priority
spanning-tree mst instance restricted-role
spanning-tree mst instance restricted-tcn

spanning-tree mst instance priority

Use this command in Interface Configuration mode for a switch port interface only to set the port priority for an MST instance (MSTI).

Use the **no** variant of this command to restore the default priority value (128).

Syntax

```
spanning-tree mst instance <instance-id> priority <priority>
no spanning-tree mst instance <instance-id> [priority]
```

Parameter	Description
<instance-id>	Specify the MSTI identifier in the range <1-15>.
<priority>	This must be a multiple of 16 and within the range <0-240>. A lower priority indicates greater likelihood of the port becoming the root port.

Default The default is 128.

Mode Interface Configuration mode for a switch port interface.

Usage This command sets the value of the priority field contained in the port identifier. The MST algorithm uses the port priority when determining the root port for the switch in the MSTI. The port with the lowest value is considered to have the highest priority and will be chosen as root port over a port - equivalent in all other aspects - but with a higher priority value.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 priority 112

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 priority
```

Related Commands

instance vlan (MSTP)
spanning-tree priority (port priority)
spanning-tree mst instance
spanning-tree mst instance path-cost
spanning-tree mst instance restricted-role
spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-role

Use this command in Interface Configuration mode for a switch port interface only to enable the restricted role for an MSTI (Multiple Spanning Tree Instance) on a switch port. Configuring the restricted role for an MSTI on a switch port prevents the switch port from becoming the root port in a spanning tree topology.

Use the **no** variant of this command to disable the restricted role for an MSTI on a switch port. Removing the restricted role for an MSTI on a switch port allows the switch port to become the root port in a spanning tree topology.

Syntax

```
spanning-tree mst instance <instance-id> restricted-role
no spanning-tree mst instance <instance-id> restricted-role
```

Parameter	Description
<instance-id>	<1-15> Specify the MST instance ID. The MST instance must have already been created using the **instance vlan (MSTP)** command.

Default The restricted role for an MSTI instance on a switch port is disabled by default.

Mode Interface Configuration mode for a switch port interface only.

Usage The root port is the port providing the best path from the bridge to the root bridge. Use this command to disable a port from becoming a root port. Use the **no** variant of this command to enable a port to become a root port. See **Spanning Tree Operation** for root port information.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3
restricted-role

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-role
```

Related Commands

instance vlan (MSTP)
spanning-tree priority (port priority)
spanning-tree mst instance
spanning-tree mst instance path-cost
spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-tcn

Use this command in Interface Configuration mode for a switch port interface only to set the restricted TCN (Topology Change Notification) value to TRUE for the specified MSTI (Multiple Spanning Tree Instance).

Use the **no** variant of this command in Interface Configuration mode to reset the restricted TCN for the specified MSTI to the default value of FALSE.

Syntax

```
spanning-tree mst instance <instance-id> restricted-tcn
no spanning-tree mst instance <instance-id> restricted-tcn
```

Parameter	Description
<instance-id>	<1-15> Specify the MST instance ID. The MST instance must have already been created using the **instance vlan (MSTP)** command.

Default The default value for restricted TCNs is FALSE, as reset with the **no** variant of this command.

Mode Interface Configuration mode for a switch port interface only.

Usage A Topology Change Notification (TCN) is a simple Bridge Protocol Data Unit (BPDU) that a bridge sends out to its root port to signal a topology change. You can configure restricted TCN between TRUE and FALSE values with this command and the **no** variant of this command.

If you configure restricted TCN to TRUE with this command then this stops the switch port from propagating received topology change notifications and topology changes to other switch ports.

If you configure restricted TCN to FALSE with the **no** variant of this command then this enables the switch port to propagate received topology change notifications and topology changes to other switch ports.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-tcn

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
                   restricted-tcn
```

Related Commands

instance vlan (MSTP)
spanning-tree priority (port priority)
spanning-tree mst instance
spanning-tree mst instance path-cost
spanning-tree mst instance restricted-role

spanning-tree path-cost

Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path for the specified port. This value then combines with others along the path to the root bridge in order to determine the total cost path value from the particular port, to the root bridge. The lower the numeric value, the higher the priority of the path. This applies when the port is the root port.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the port's path cost for the CIST.

Syntax

```
spanning-tree path-cost <pathcost>
no spanning-tree path-cost
```

Parameter	Description
<pathcost>	<1-200000000> The cost to be assigned to the port.

Default The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 and IEEE 802.1d-2004 standards.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2, 000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode Interface Configuration mode for switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 123
```

spanning-tree portfast (STP)

Use this command in Interface Configuration mode for a switch port interface only to set a port as an edge-port. The portfast feature enables a port to rapidly move to the forwarding state, without having first to pass through the intermediate spanning tree states. This command has the same effect as the **spanning-tree edgeport (RSTP and MSTP)** command, but the configuration displays differently in the output of some show commands.

Note

You can run either of two additional parameters with this command. To simplify the syntax these are documented as separate commands. See the following additional portfast commands:

- **spanning-tree portfast bpdu-filter** command on page 19.62
- **spanning-tree portfast bpdu-guard** command on page 19.64.

You can obtain the same effect by running the **spanning-tree edgeport (RSTP and MSTP)** command. However, the configuration output may display differently in some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax

```
spanning-tree portfast

no spanning-tree portfast
```

Default Not an edge port.

Mode Interface Configuration mode for a switch port interface only.

Usage Portfast makes a port move from a blocking state to a forwarding state, bypassing both listening and learning states. The portfast feature is meant to be used for ports connected to end-user devices not switches. Enabling portfast on ports that are connected to a workstation or server allows devices to connect to the network without waiting for spanning-tree to converge.

For example, you may need hosts to receive a DHCP address quickly and waiting for STP to converge would cause the DHCP request to time out. Ensure you do not use portfast on any ports connected to another switch to avoid creating a spanning-tree loop on the network.

Use this command on a switch port that connects to a LAN with no other bridges attached. An edge port should never receive BPDUs. Therefore if an edge port receives a BPDU, the portfast feature takes one of three actions.

- Cease to act as an edge port and pass BPDUs as a member of a spanning tree network (**spanning-tree portfast (STP)** command disabled).
- Filter out the BPDUs and pass only the data and continue to act as a edge port (**spanning-tree portfast bpdu-filter** command enabled).
- Block the port to all BPDUs and data (**spanning-tree portfast bpdu-guard** command enabled).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast
```

Related Commands

spanning-tree edgeport (RSTP and MSTP)
show spanning-tree
spanning-tree portfast bpdu-filter
spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-filter

This command sets the bpdu-filter feature and applies a filter to any BPDUs (Bridge Protocol Data Units) received. Enabling this feature ensures that configured ports will not transmit any BPDUs and will ignore (filter out) any BPDUs received. BPDU Filter is not enabled on a port by default.

Using the **no** variant of this command to turn off the bpdu-filter, but retain the port's status as an enabled port. If the port then receives a BPDU it will change its role from an **edge-port** to a **non edge-port**.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-filter

no spanning-tree portfast bpdu-filter
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-filter {default|disable|enable}

no spanning-tree portfast bpdu-filter
```

Parameter	Description	
`bpdu-filter`	A port that has bpdu-filter enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole switch, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU filter.
	`enable`	Turns on BPDU filter.

Default BPDU Filter is not enabled on any ports by default.

Mode Global Configuration and Interface Configuration

Usage This command filters the BPDUs and passes only data to continue to act as an edge port. Using this command in Global Configuration mode applies the portfast bpdu-filter feature to all ports on the switch. Using it in Interface mode applies the feature to a specific port, or range of ports.The command will operate in both RSTP and MSTP networks.

Use the **show spanning-tree** command to display status of the bpdu-filter parameter for the switch ports.

Example To enable STP BPDU filtering in Global Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-filter
```

To enable STP BPDU filtering in Interface Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-filter enable
```

Related Commands
spanning-tree edgeport (RSTP and MSTP)
show spanning-tree
spanning-tree portfast (STP)
spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-guard

This command applies a BPDU (Bridge Protocol Data Unit) guard to the port. A port with the bpdu-guard feature enabled will block all traffic (BPDUs and user data), if it starts receiving BPDUs.

Use this command in Global Configuration mode to apply BPDU guard to all ports on the switch. Use this command in Interface mode for an individual interface or a range of interfaces specified. BPDU Guard is not enabled on a port by default.

Use the **no** variant of this command to disable the BPDU Guard feature on a switch in Global Configuration mode or to disable the BPDU Guard feature on a port in Interface mode.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-guard

no spanning-tree portfast bpdu-guard
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-guard {default|disable|enable}

no spanning-tree portfast bpdu-guard
```

Parameter	Description	
`bpdu-guard`	A port that has bpdu-guard turned on will enter the STP blocking state if it receives a BPDU. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole switch, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU guard.
	`enable`	Turns on BPDU guard and will also set the port as an edge port.

Default BPDU Guard is not enabled on any ports by default.

Mode Global Configuration or Interface Configuration

Usage This command blocks the port(s) to all BPDUs and data when enabled. BPDU Guard is a port-security feature that changes how a portfast-enabled port behaves if it receives a BPDU. When **bpdu-guard** is set, then the port shuts down if it receives a BPDU. It does not process the BPDU as it is considered suspicious. When **bpdu-guard** is not set, then the port will negotiate spanning-tree with the device sending the BPDUs. By default, bpdu-guard is not enabled on a port.

You can configure a port disabled by the bpdu-guard to re-enable itself after a specific time interval. This interval is set with the **spanning-tree errdisable-timeout interval** command on page 19.43. If you do not use the **errdisable-timeout** feature, then you will need to manually re-enable the port by using the **no shutdown** command.

Use the **show spanning-tree** command on page 19.14 to display the switch and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of bpdu-guard.

Example To enable STP BPDU guard in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

To enable STP BPDU guard in Interface Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-guard enable
```

Related Commands
spanning-tree edgeport (RSTP and MSTP)
show spanning-tree
spanning-tree portfast (STP)
spanning-tree portfast bpdu-filter

spanning-tree priority (bridge priority)

Use this command to set the bridge priority for the switch. A lower priority value indicates a greater likelihood of the switch becoming the root bridge.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-61440> The bridge priority, which will be rounded to a multiple of 4096.

Default The default priority is 32678.

Mode Global Configuration

Usage To force a particular switch to become the root bridge use a lower value than other switches in the spanning tree.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree priority 4096
```

Related Commands **spanning-tree mst instance priority**
show spanning-tree

spanning-tree priority (port priority)

Use this command in Interface Configuration mode for a switch port interface only to set the port priority for port. A lower priority value indicates a greater likelihood of the port becoming part of the active topology.

Use this command for RSTP, STP, or MSTP. When the device is in MSTP mode, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-240>, in increments of 16. The port priority, which will be rounded down to a multiple of 16.

Default The default priority is 128.

Mode Interface Configuration mode for a switch port interface only.

Usage To force a port to be part of the active topology (for instance, become the root port or a designated port) use a lower value than other ports on the device. (This behavior is subject to network topology, and more significant factors, such as bridge ID.)

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree priority 16
```

Related Commands

spanning-tree mst instance priority
spanning-tree priority (bridge priority)
show spanning-tree

spanning-tree restricted-role

Use this command in Interface Configuration mode for a switch port interface only to restrict the port from becoming a root port.

Use the **no** variant of this command to disable the restricted role functionality.

Syntax

```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Default The restricted role is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command in Interface Configuration mode for a switch port interface only to prevent TCN (Topology Change Notification) BPDUs (Bridge Protocol Data Units) from being sent on a port. If this command is enabled, after a topology change a bridge is prevented from sending a TCN to its designated bridge.

Use the **no** variant of this command to disable the restricted TCN functionality.

Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Default The restricted TCN is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-tcn
```

spanning-tree transmit-holdcount

Use this command to set the maximum number of BPDU transmissions that are held back.

Use the **no** variant of this command to restore the default transmit hold-count value.

Syntax

```
spanning-tree transmit-holdcount
no spanning-tree transmit-holdcount
```

Default Transmit hold-count default is 3.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree transmit-holdcount
```

undebug mstp

This command applies the functionality of the **no debug mstp (RSTP and STP)** command.

Chapter 20: Link Aggregation Introduction and Configuration

Introduction and Overview 20.2
Static and Dynamic (LACP) Link Aggregation 20.3
Static Channel Groups 20.3
Dynamic (LACP) Channel Groups 20.3
Link Aggregation Control Protocol (LACP) 20.3
Configuring an LACP Channel Group 20.5
Minimal LACP Group Configuration 20.8
Configuring a Static Channel Group 20.9

Introduction and Overview

This chapter contains two sample Link Aggregation Control Protocol (LACP), or dynamic channel group, configurations and a sample static channel group configuration.

Link aggregation is the process where two or more ports in an Ethernet switch are combined together to operate as a single virtual port.

Link aggregation is a key component in resilient network design, since it increases the available bandwidth between network devices and it provides continuity of connectivity if one link is broken between network devices.

By aggregating two or more links together, you can increase the bandwidth between neighboring devices since this is effectively additive, where two links give up to twice the bandwidth of one link. Having more than one link to a neighboring device provides connectivity if one of the links break, where a feature of this resiliency is the speed at which link aggregation reacts to the change of link status in a matter of millisecond.

A link aggregation can only exist between a pair of neighboring switches, where the switch ports that are aggregated on one switch cannot be connected to switch ports that are not aggregated on the other switch. A switch can have multiple link aggregations to different neighbors, even to the same neighbor if the network is loop protected.

To see details about the commands used to configure dynamic (LACP) and static Link aggregation, see **Chapter 21, Link Aggregation Commands**.

For a brief overview of static and dynamic link aggregation (LACP), see **Static and Dynamic (LACP) Link Aggregation**.

Static and Dynamic (LACP) Link Aggregation

Channels, either static or dynamic LACP, increase reliability by distributing the data path over more than one physical link. Channels must be configured on both ends of a link or network loops may result. Ports in a channel group need not be contiguous. A mirror port cannot be a member of either a static or a dynamic channel group.

Aggregation criteria

For individual links to be aggregated into a channel group they must:

- originate on the same device or stack
- terminate on the same device or stack
- be members of the same VLANs (**vlan** command on page 17.33)
- have the same data rate (**speed** command on page 15.43)
- share the same admin port key (assigned by using the **channel-group** command on page 21.3 command)
- be operating in full duplex mode (**duplex** command on page 15.8)

The hardware must also be capable and have the capacity to handle the number of links to be aggregated.

Static Channel Groups

A static channel group, also known as a static aggregator, enables a number of ports to be manually configured to form a single logical connection of higher bandwidth. By using static channel groups you increase channel reliability by distributing the data path over more than one physical link. Static channel groups are best used in simpler environments, usually where neighbor switches are close together, situated within the same rack, so that you can easily ensure that the correct statically aggregated ports are connected together.

For a static channel group configuration example see the **Configuring a Static Channel Group** section in this chapter. For details of static channel group commands, such as the **static-channel-group** command, see **Chapter 21, Link Aggregation Commands**.

Dynamic (LACP) Channel Groups

A LACP channel group, also known as an etherchannel, a LACP aggregator, or a dynamic channel group, enables a number of ports to be dynamically combined to form a single higher bandwidth logical connection. LACP channel groups are best used for complex environments, typically long-distance links, to detect failure between neighbor switches.

For LACP configuration examples see **Configuring an LACP Channel Group** and **Minimal LACP Group Configuration** sections in this chapter. For details of LACP channel group commands, such as the **channel-group** command, see **Chapter 21, Link Aggregation Commands**.

Link Aggregation Control Protocol (LACP)

LACP is based on the IEEE Standard 802.3ad. It allows bundling of several physical ports to form a single logical channel providing enhanced performance and resiliency. The aggregated channel is viewed as a single link by each switch. Spanning tree also views the channel as one interface and not as multiple interfaces. When there is a failure in one physical port, the other ports stay up and there is no disruption.

Note

AlliedWare Plus™ supports IEEE 802.3ad link aggregation and uses the Link Aggregation Control Protocol (LACP). LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).

Note

Link aggregation does not necessarily achieve exact load balancing across the links. The load sharing algorithm is designed to ensure that any given data flow always goes down the same link. It also aims to spread data flows across the links as evenly as possible.

Link aggregation hashes one or more of the source and destination MAC address, IP address and UDP/TCP ports to select a link on which to send a packet. So packet flow between a pair of hosts always takes the same link inside the Link Aggregation Group (LAG). The net effect is that the bandwidth for a given packet stream is restricted to the speed of one link in the LAG.

For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.

LACP operates where systems are connected over multiple communications links. Once LACP has been initially configured and enabled, it automatically aggregates the ports that have been assigned to a channel group, if possible. LACP continues to monitor these groups and dynamically adds or removes links to them as network changes occur.

LACP achieves this by determining:

- which ports are under LACP control (**channel-group** command on page 21.3)
- whether each port is in LACP active or LACP passive mode (**channel-group** command on page 21.3)
- which system has the highest LACP priority (**lacp system-priority** command on page 21.8)
- the LACP priority of ports (**lacp port-priority** command on page 21.7)
- whether the LACP timeout is short or long (**lacp timeout** command on page 21.9)

Channel group identification

In order to identify particular channel groups, each group is assigned a link aggregation identifier called a **lag ID**. The lag ID comprises the following components for both the local system (called the Actor) followed by their equivalent components for the remote system (called the Partner):

- system identifier - the MAC address of the system
- port key - An identifier - created by the LACP software
- port priority - set by the **lacp port-priority** command on page 21.7
- port number - determined by the device connection

The lag ID can be displayed for each aggregated link by entering the **show etherchannel** command on page 21.13.

Configuring an LACP Channel Group

The following example shows how to configure three links between two Allied Telesis managed Layer 3 Switches. The three links are assigned the same administrative key (1), so that they aggregate to form a single channel (1). They are viewed by the STP as one interface.

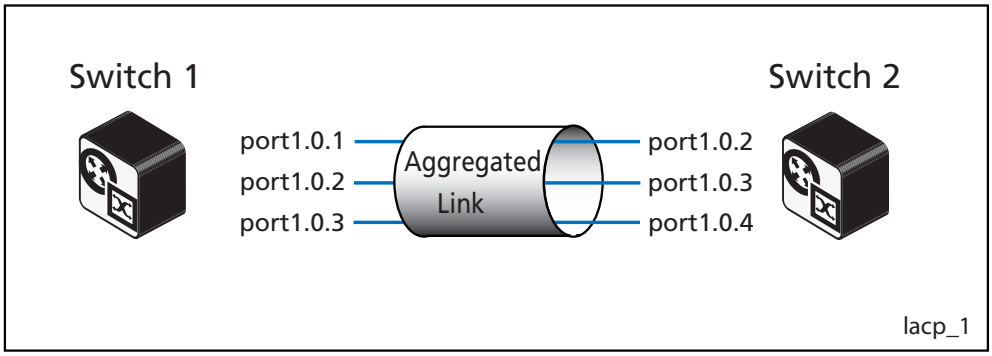


Table 20-1: Switch 1 configuration

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `lacp system-priority 20000`	Set the system priority of this switch. This priority is used to determine which switch in the system is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority. Switch 1 has a higher priority than Switch 2 in this configuration.
`awplus(config)#` `interface port1.0.1`	Enter the Interface Configuration mode to configure port `1.0.1`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and return to the Global Configure mode.
`awplus(config)#` `interface port1.0.2`	Enter the Interface Configuration mode to configure port `1.0.2`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.

Table 20-1: Switch 1 configuration (cont.)

`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and return to the Global Configure mode.
`awplus(config)#` `interface port1.0.3`	Enter the Interface Configuration mode to configure port `1.0.3`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.
`awplus(config-if)#` `interface po1`	Select the dynamic aggregator logical interface created for channel-group 1 named `po1`.

Table 20-2: Switch 2 configuration

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `lacp system-priority 3000`	Set the system priority of this switch. This priority is used to determine which switch in the system is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority. Switch 2 has a lower priority than Switch 1 in this configuration.
`awplus(config)#` `interface port1.0.2`	Enter the Interface Configuration mode to configure port `1.0.2`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.
`awplus(config-if)#` `exit`	Exit the Interface mode and return to the Configure mode.
`awplus(config)#` `interface port1.0.3`	Enter the Interface mode to configure port `1.0.3`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.

Table 20-2: Switch 2 configuration

`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and return to the Global Configuration mode.
`awplus(config)#` `interface port1.0.4`	Enter the Interface Configuration mode to configure port `1.0.4`.
`awplus(config-if)#` `channel-group 1 mode active`	Add this interface to a channel group `1` and enable link aggregation so that it may be selected for aggregation by the local system.
`awplus(config-if)#` `interface po1`	Select the dynamic aggregator logical interface created for channel-group 1 named `po1`.

Commands used

lacp system-priority
channel-group

Validation commands

show lacp sys-id
show port etherchannel
show etherchannel
show etherchannel detail

Minimal LACP Group Configuration

For details of LACP channel group commands, see **Chapter 21, Link Aggregation Commands**.

The following minimal LACP group configuration example creates LACP channel group 2 and enables link aggregation on switch ports `1.0.1` and `1.0.2` within this channel group. Note that all aggregated ports must belong to the same VLAN.

`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `interface port1.0.1-port1.0.2`	Enter the Interface Configuration mode for the switch ports to aggregate into the channel group.
`awplus(config-if)#` `channel-group 2 mode active`	Assign the switch ports to channel group `2` in active mode. This creates the channel group.
`awplus(config-if)#` `interface po2`	Select the dynamic aggregator logical interface created for channel-group 2 named `po2`.

Commands used

channel-group

Validation commands

show static-channel-group

Configuring a Static Channel Group

For details of LACP channel group commands, see **Chapter 21, Link Aggregation Commands**.

The following example creates a static channel group and adds switch ports `1.0.1` and `1.0.2`.

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `interface port1.0.1`	Enter the Interface Configuration mode to configure port `1.0.1`.
`awplus(config-if)#` `static-channel-group 2`	Add port `1.0.1` to static-channel-group `2`.
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and return to the Global Configuration mode.
`awplus(config)#` `interface port1.0.2`	Enter the Interface Configuration mode to configure port `1.0.2`.
`awplus(config-if)#` `static-channel-group 2`	Add port `1.0.2` to static-channel-group `2`.
`awplus(config-if)#` `interface sa2`	Select the static aggregator logical interface created for static-channel-group 2 named `sa2`.

Commands used

static-channel-group

Validation commands

show static-channel-group

Chapter 21: Link Aggregation Commands

Introduction 21.2
Command List 21.3
channel-group 21.3
clear lacp counters 21.5
debug lacp 21.6
lacp port-priority 21.7
lacp system-priority 21.8
lacp timeout 21.9
show debugging lacp 21.11
show diagnostic channel-group 21.12
show etherchannel 21.13
show etherchannel detail 21.14
show etherchannel summary 21.15
show lacp sys-id 21.16
show lacp-counter 21.17
show port etherchannel 21.18
show static-channel-group 21.19
static-channel-group 21.20
undebug lacp 21.22

Introduction

This chapter provides an alphabetical reference of commands used to configure a static channel group (static aggregator) and dynamic channel group (LACP channel group, etherchannel or LACP aggregator). Link aggregation is also sometimes referred to as channeling.

Note

AlliedWare Plus™ supports IEEE 802.3ad link aggregation and uses the Link Aggregation Control Protocol (LACP). LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).

Note

Link aggregation does not necessarily achieve exact load balancing across the links. The load sharing algorithm is designed to ensure that any given data flow always goes down the same link. It also aims to spread data flows across the links as evenly as possible.

Link aggregation hashes one or more of the source and destination MAC address, IP address and UDP/TCP ports to select a link on which to send a packet. So packet flow between a pair of hosts always takes the same link inside the Link Aggregation Group (LAG). The net effect is that the bandwidth for a given packet stream is restricted to the speed of one link in the LAG.

For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.

For a description of static and dynamic link aggregation (LACP), see **"Configuring an LACP Channel Group" on page 20.5**. For an LACP configuration example, see **Chapter 20, Link Aggregation Introduction and Configuration**.

Command List

channel-group

Use this command to add the device port to a dynamic channel group specified by the dynamic channel group number, and set its mode. This command enables LACP link aggregation on the device port, so that it may be selected for aggregation by the local system. Dynamic channel groups are also known as LACP channel groups, LACP aggregators or etherchannels.

You can create up to 32 dynamic (LACP) channel groups (and up to 96 static channel groups).

Use the **no** variant of this command to turn off link aggregation on the device port. You will be returned to Global Configuration mode from Interface Configuration mode.

Syntax

```
channel-group <dynamic-channel-group-number> mode {active|passive}
no channel-group
```

Parameter	Description
<dynamic-channel-group-number>	<1-32> Specify a dynamic channel group number for an LACP link. You can create up to 32 dynamic (LACP) channel groups (as well as up to 96 static channel groups).
active	Enables initiation of LACP negotiation on a port. The port will transmit LACP dialogue messages whether or not it receives them from the partner system.
passive	Disables initiation of LACP negotiation on a port. The port will only transmit LACP dialogue messages if the partner systems is transmitting them, i.e., the partner is in the active mode.

Mode Interface Configuration

Usage All the device ports in a channel-group must belong to the same VLANs, have the same tagging status, and can only be operated on as a group. All device ports within a channel group must have the same port speed and be in full duplex mode.

Once the LACP channel group has been created, it is treated as a device port, and can be referred to in most other commands that apply to device ports.

To refer to an LACP channel group in other LACP commands, use the channel group number. To specify an LACP channel group (LACP aggregator) in other commands, prefix the channel group number with **po**. For example, 'po2' refers to the LACP channel group with channel group number 2.

For more on LACP, see **"Dynamic (LACP) Channel Groups" on page 20.3** and **Chapter 20, Link Aggregation Introduction and Configuration**.

Examples

To add device `port1.0.6` to a newly created LACP channel group 2 use the commands below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
```

To remove device `port1.0.6` from any created LACP channel groups use the command below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no channel-group
awplus(config)#
```

To reference the pre-defined LACP channel group 2 as an interface, apply commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface port.1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface po2
awplus(config-if)#
```

Related Commands

show etherchannel
show etherchannel detail
show etherchannel summary
show port etherchannel

clear lacp counters

Use this command to clear all counters of all present LACP aggregators (channel groups) or a given LACP aggregator.

Syntax `clear lacp [<1-32>] counters`

Parameter	Description
<1-32>	Channel-group number.

Mode Privileged Exec

Example

```
awplus# clear lacp 2 counters
```

debug lacp

Use this command to enable all LACP troubleshooting functions.

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

Syntax

```
debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
no debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
```

Parameter	Description
`all`	Turn on all debugging for LACP.
`cli`	Specifies debugging for CLI messages. Echoes commands to the console.
`event`	Specifies debugging for LACP events. Echoes events to the console.
`ha`	Specifies debugging for HA (High Availability) events. Echoes High Availability events to the console.
`packet`	Specifies debugging for LACP packets. Echoes packet contents to the console.
`sync`	Specified debugging for LACP synchronization. Echoes synchronization to the console.
`timer`	Specifies debugging for LACP timer. Echoes timer expiry to the console.
`detail`	Optional parameter for LACP timer-detail. Echoes timer start/stop details to the console.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug lacp timer detail
awplus# debug lacp all
```

Related Commands **show debugging lacp**
undebug lacp

lacp port-priority

Use this command to set the priority of a device port. Ports are selected for aggregation based on their priority, with the higher priority (numerically lower) ports selected first.

Use the **no** variant of this command to reset the priority of port to the default.

Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameter	Description
<1-65535>	Specify the LACP port priority.

Default The default is 32768.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# lacp port-priority 34
```

lacp system-priority

Use this command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups.

Use the **no** variant of this command to reset the system priority of the local system to the default.

Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameter	Description
<1-65535>	LACP system priority. Lower numerical values have higher priorities.

Default The default is 32768.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# lacp system-priority 6700
```

lacp timeout

Use this command to set the short or long timeout on a port. Ports will time out of the aggregation if three consecutive updates are lost.

Syntax `lacp timeout {short|long}`

Parameter	Description
`timeout`	Number of seconds before invalidating a received LACP data unit (DU).
`short`	LACP short timeout. The **short** timeout value is **1** second.
`long`	LACP long timeout. The **long** timeout value is **30** seconds.

Default The default is **long** timeout (30 seconds).

Mode Interface Configuration

Usage This command enables the device to indicate the rate at which it expects to receive LACPDUs from its neighbor.

If the timeout is set to **long**, then the device expects to receive an update every **30** seconds, and this will time a port out of the aggregation if no updates are seen for 90 seconds (i.e. 3 consecutive updates are lost).

If the timeout is set to **short**, then the device expects to receive an update every second, and this will time a port a port out of the aggregation if no updates are seen for 3 seconds (i.e. 3 consecutive updates are lost).

The device indicates its preference by means of the '`Timeout`' field in the '`Actor`' section of its LACPDUs. If the '`Timeout`' field is set to 1, then the device has set the **short** timeout. If the '`Timeout`' field is set to 0, then the device has set the **long** timeout.

Setting the **short** timeout enables the device to be more responsive to communication failure on a link, and does not add too much processing overhead to the device (1 packet per second).

Note It is not possible to configure the rate that the device sends LACPDUs; the device must send at the rate which the neighbor indicates it expects to receive LACPDUs.

Examples The following commands set the LACP long timeout period for 30 seconds on `port1.0.2`.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout long
```

The following commands set the LACP short timeout for 1 second on `port1.0.2`.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout short
```

show debugging lacp

Use this command to display the LACP debugging option set.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show debugging lacp
```

Mode

User Exec and Privileged Exec

Example

```
awplus# show debugging lacp
```

Output

Figure 21-1: Example output from the show debugging lacp command

```
LACP debugging status:
 LACP timer debugging is on
 LACP timer-detail debugging is on
 LACP cli debugging is on
 LACP packet debugging is on
 LACP event debugging is on
 LACP sync debugging is on
```

Related Commands

debug lacp

show diagnostic channel-group

This command displays dynamic and static channel group interface status information. The output of this command is useful for Allied Telesis authorized service personnel for diagnostic purposes.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show diagnostic channel-group`

Mode User Exec and Privileged Exec

Example

```
awplus# show diagnostic channel-group
```

Output **Figure 21-2: Example output from the show diagnostic channel-group command**

```
awplus#show diagnostic channel-group

Channel Group Info based on NSM:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503     port1.0.15   5015     No
     sa3        4503     port1.0.18   5018     No
     po1        4601     port1.0.7    5007     No
     po1        4601     port1.0.8    5008     No
     po1        4601     port1.0.9    5009     No


Channel Group Info based on HSL:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


Channel Group Info based on IPIFWD:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


Channel Group Info based on HW:
Note: Pos - position in hardware table
      Only entries from first device are displayed.
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


No error found
```

Related Commands **show tech-support**

show etherchannel

Use this command to display information about a LACP channel specified by the channel group number.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **thrash limiting** parameter of the **thrash-limiting** command on page 15.46 is set to **vlan disable**, the output will also show the VLANs on which thrashing is detected.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show etherchannel [<1-32>]`

Parameter	Description
<1-32>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel 2
```

Output **Figure 21-3:**

Figure 21-4: Example output from the show etherchannel command for a particular channel

```
% Lacp Aggregator: po1
 Thrash-limiting
 Status Vlan Thrashing Detected, Action vlan-disable 60(s)
 Thrashing Vlans 1 2 3 4 5
% Member:
   port1.0.4
   port1.0.6
```

show etherchannel detail

Use this command to display detailed information about all LACP channels.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show etherchannel detail`

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel detail
```

Output **Figure 21-5: Example output from the show etherchannel detail command**

```
Aggregator po1 (IfIndex: 4501)
 Mac address: 00:00:cd:24:fd:29
 Admin Key: 0001 - Oper Key 0001
 Receive link count: 1 - Transmit link count: 0
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-24-da-a7
  Link: port1.0.1 (IfIndex: 5001) disabled
  Link: port1.0.2 (IfIndex: 5002) sync: 1
Aggregator po2 (IfIndex: 4502)
 Mac address: 00:00:cd:24:fd:29
 Admin Key: 0002 - Oper Key 0002
 Receive link count: 1 - Transmit link count: 0
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-24-da-a7
  Link: port1.0.6 (IfIndex: 5007) disabled
```

show etherchannel summary

Use this command to display a summary of all LACP channels.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show etherchannel summary
```

Mode

User Exec and Privileged Exec

Example

```
awplus# show etherchannel summary
```

Output

Figure 21-6: Example output from the show etherchannel summary command

```
% Aggregator po1
%  Admin Key: 0001 - Oper Key 0001
%   Link: port1.0.1 (5001) disabled
%   Link: port1.0.2 (5002) sync: 1
% Aggregator po2
%  Admin Key: 0002 - Oper Key 0002
%   Link: port1.0.6 (5007) disabled
```

show lacp sys-id

Use this command to display the LACP system ID and priority.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show lacp sys-id
```

Mode

User Exec and Privileged Exec

Example

```
awplus# show lacp sys-id
```

Output

Figure 21-7: Example output from the show lacp sys-id command

```
System Priority: 0x8000 (32768)
MAC Address: 0200.0034.5684
```

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show lacp-counter [<1-32>]`

Parameter	Description
<1-32>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show lacp-counter 2
```

Output **Figure 21-8: Example output from the show lacp-counter command**

```
% Traffic statistics
Port          LACPDUs         Marker         Pckt err
            Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po2 (IfIndex: 4604)
port1.0.2   0       0       0       0       0       0
```

show port etherchannel

Use this command to show LACP details of the device port specified.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show port etherchannel <port>`

Parameter	Description
<port>	Name of the device port to display LACP information about.

Mode User Exec and Privileged Exec

Example

```
awplus# show port etherchannel port1.0.1
```

Output **Figure 21-9: Example output from the show port etherchannel command**

```
Link: port1.0.1 (5001) Aggregator: po1 (4501)
Receive machine state: Current
Periodic Transmission machine state: Fast periodic
Mux machine state: Collecting/Distributing
Actor Information:                    Partner Information:
  Selected ................ Selected     Partner Sys Priority ............ 0
  Physical Admin Key ..... 1            Partner System .. 00-00-00-00-00-00
  Port Key ............... 5            Port Key ........................ 0
  Port Priority ..... 32768             Port Priority ................... 0
  Port Number ..,,,,,,.... 5001         Port Number ..................... 0
  Mode ..................... Active     Mode ....................... Passive
  Timeout ..................... Long    Timeout ..................... Short
  Individual ................... Yes    Individual ..................... Yes
  Synchronised ................. Yes    Synchronised ................... Yes
  Collecting ................... Yes    Collecting ..................... Yes
  Distributing ................. Yes    Distributing ................... Yes
  Defaulted .................... Yes    Defaulted ...................... Yes
  Expired ...................... No     Expired ........................ No
```

show static-channel-group

Use this command to display all configured static channel groups and their corresponding member ports. Note that a static channel group is the same as a static aggregator.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **thrash limiting** parameter of the **thrash-limiting** command on page 15.46 is set to **vlan disable**, the output will also show the VLANs on which thrashing is detected.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show static-channel-group
```

Mode

User Exec and Privileged Exec

Example

```
awplus#  show static-channel-group
```

Output

Figure 21-10: Example output from the show static-channel-group command

```
% LAG Maximum        : 128
% LAG Static  Maximum: 96
% LAG Dynamic Maximum: 32
% LAG Static  Count  : 2
% LAG Dynamic Count  : 2
% LAG Total   Count  : 4
% Static Aggregator: sa2
% Member:
   port1.0.1
% Static Aggregator: sa3
% Member:
   port1.0.2
```

Related Commands

static-channel-group

static-channel-group

Use this command to create a static channel group, also known as a static aggregator, or add a member port to an existing static channel group.

You can create up to 96 static channel groups (and up to 32 dynamic channel groups).

Use the **no** variant of this command to remove the device port from the static channel group.

Syntax

```
static-channel-group <static-channel-group-number>
no static-channel-group
```

Parameter	Description
<static-channel-group-number>	<1-96> Static channel group number.

Mode Interface Configuration

Usage This command adds the device port to the static channel group with the specified channel group number. If the channel group does not exist, it is created, and the port is added to it. The **no** prefix detaches the port from the static channel group. If the port is the last member to be removed, the static channel group is deleted.

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Once the static channel group has been created, it is treated as a device port, and can be referred to in other commands that apply to device ports.

To refer to a static channel group in other static channel group commands, use the channel group number. To specify a static channel group in other commands, prefix the channel group number with **sa**. For example, 'sa2' refers to the static channel group with channel group number 2.

For more on static channel groups, see **"Static Channel Groups" on page 20.3** and **Chapter 20, Link Aggregation Introduction and Configuration**.

Examples To define a static channel group on a device port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# static-channel-group 2
```

To reference the pre-defined static channel group 2 as an interface apply the example commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface port.1.0.6
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)#
```

Related Commands **show static-channel-group**

undebug lacp

This command applies the functionality of the **no debug lacp** command on page 21.6.

Chapter 22: Power over Ethernet Introduction

Introduction 22.2
PoE Standards 22.2
PoE (all standards) 22.3
PoE (IEEE 802.3af) 22.3
Enhanced PoE 22.3
PoE+ (IEEE 802.3at) 22.3
Differences Between PoE and PoE+ 22.5
LLDP-MED (TIA-1057) with PoE+ (IEEE 802.3at) 22.5
PoE and PoE+ Applications 22.5
Power Device (PD) Discovery 22.5
Power Classes 22.6
Power through the Cable 22.7
Cable Types 22.8
Static and Automatic Power Allocation 22.8
PoE and PoE+ Implementation 22.9
Power Capacity 22.9
PoE Port Allocation and Distribution 22.9
Power Threshold 22.9
Negotiating Power Requirements 22.10
PoE Port Management 22.10
Powered Device (PD) Detection 22.10
Port Prioritization 22.10
Software Monitoring 22.12
PoE and PoE+ Configuration 22.13
Add a Description for a PoE or PoE+ Port 22.13
Configuring Capacity and Priority on a PoE or PoE+ Port 22.14
Remotely Monitoring Power for all Connected PDs 22.15

Introduction

This chapter provides an introduction to Power over Ethernet (PoE) technology, the PoE standards, PoE devices, and how to configure PoE on your switch. The AT-GS924MPX and AT-GS948MPX models are PoE capable.

For information about the PoE commands available on your switch, see **Chapter 23, Power over Ethernet Commands**.

PoE is a method of supplying power to network devices by utilizing the same cabling used to carry network traffic. PoE is appropriate for devices that have a low power consumption (termed Powered Devices) such as IP phones and security cameras etc. A number of standards have been created to define PoE connectivity. Two PoE standards are presently defined by the Institute of Electrical and Electronics Engineers (IEEE), these are: IEEE 802.3af and IEEE 802.3at.

In addition to the formal PoE methods defined by the IEEE, there are also legacy industry methods for supplying power over Ethernet cabling. For details of legacy support see the command, **power-inline allow-legacy** command on page 23.5.

PoE Standards

PoE is formally defined by the following standards: **formal** (defined by the IEEE), and **de facto** (industry developed):

- IEEE 802.3af Power Ethernet standard
  - « Approved 2003.
  - « Supplies 15.94 W of power of which 12.95 W is available to each powered device.
  - « Superseded by IEEE IEEE802.3at.
  - « Fully supported on the AT-GS924MPX and AT-GS948MPXswitches

For more information on this standard, refer to **"PoE (IEEE 802.3af)" on page 22.3**.

- Enhanced PoE
  - « Industry standard introduced after the IEEE 802.af. It provides more power (20 W) than defined by IEEE 802.3.af but less than the power (30 W) defined by IEEE 802.3.at.
  - « Compliance with this method is provided on the AT-GS924MPX and AT-GS948MPX switches on a best effort basis.
  - « For more information on this standard, refer to **"Enhanced PoE" on page 22.3**.
- IEEE 802.3at Power Ethernet standard (commonly known as PoE+)
  - « Approved 2009.
  - « Supplies 30 W of power of which 25.5 W is available to each powered device.
  - « For more information on this method, refer to **"PoE+ (IEEE 802.3at)" on page 22.3**.
  - « Fully supported on the AT-GS924MPX and AT-GS948MPX switches.

PoE (all standards)

The general objective that is common to all PoE methods described in this document is to distribute both data and cable over the same cabling that is used for transmitting Ethernet based data. This eliminates the need for having one set of cables and outlets for data, and another set for power. Also, because the voltage and power requirements are much lower than for mains powered devices, the cabling and installation costs are significantly reduced.

Power Sourcing Equipment (PSE) such as an Ethernet LAN switch or router, supplies power to the cable together with the data. **Powered Devices (PDs)** such as Wireless Access Points or an IP Phones, receive power and data over this same cabling. The PSE employs various methods of power classification (depending on the standard) for detecting compatible PDs from non-compatible devices and will only provide the maximum power limit to compatible PDs, based on their PoE device class. The PSE continuously monitors the PDs and stops providing power when it is no longer requested or it detects an overload or short circuit condition on a port.

PoE (IEEE 802.3af)

The IEEE 802.3at-2003 standard specifies how power is distributed along with data on twisted pair Ethernet LAN cables. The standard specifies that the PSE is able to supply up to 15.4 watts (W) of power (at a nominal 48 VDC), with the full 100 m cable length, is then able to utilize 12.95 W. The difference between these power levels (15.4 -12.98) allows for power loss within the cabling. This figure is approximate and will vary with the cable length and quality. The IEEE 802.3af physical layer classification is a static power allocation based on power bands for power management.

Enhanced PoE

Enhanced was developed prior to IEEE802.3at standard to provide more power the PDs than was currently offered by the old 802.3af standard. Enhanced PoE supplied between 15.4 W and 20 W per port at 48 VDC. Typically, these PD would be used for applications such as building security and video surveillance. Note that IEEE 802.3at standard PoE+ PDs that require 56 VDC cannot use Enhanced PoE PSEs instead of IEEE 802.3at standard PoE+ PSEs. Enhanced PoE PSEs cannot replace IEEE 802.3at standard PSEs when using any PoE+ PDs.

PoE+ (IEEE 802.3at)

The IEEE 802.3at-2009 standard specifies how power is distributed together with data on twisted pair Ethernet LAN cables. PoE+ supplies the higher power required by a new generation of network attached devices. These devices, such as, multiple radio IEEE 802.11n wireless access points, powered pan tilt and zoom IP security cameras, thin clients, door locks, touch screen displays, and video phones frequently require more than the 12.9 W (at a nominal 54 VDC) available under the IEEE 802.3af standard. The IEEE 802.3at specification provides for up to 30 W of power at the PSE, of which 25.5 W is available to the PD.

The standard also requires that PDs support a flexible Layer 2 power classification method using Link Layer Discovery Protocol Media Endpoint Devices (LLDP-MED). The use of LLDP-MED for power classification provides PoE power allocation in steps of 1 watt, along with an ability to reallocate power, for improved power allocation and management between the PSE and PD. For more information see **"LLDP-MED (TIA-1057) with PoE+ (IEEE 802.3at)" on page 22.5**. The IEEE 802.3at specification is backwards compatible with the IEEE 802.3af specification. Devices that support the IEEE 802.3at specification are optimized to operate with IEEE 802.3at PSEs to support dynamic power management. PSEs that support the IEEE 802.3af specification can still interoperate with IEEE 802.3at compliant PDs, providing that the PD can operate using 12.95 W of power. However, these PDs will operate without the dynamic power allocation and management feature.

Differences Between PoE and PoE+

The major differences between the IEEE 802.3af (PoE) and the IEEE 802.3at (PoE+) standards relate to the power that the PDs are allowed to consume, and the ability to dynamically manage the power supplied to each PD. The following table summarizes the major differences in terms of their applied voltages and power ratings.

Standard	Voltage DC at PSE	Cabling	Power Supplied by PSE	Power Available to PD	Nominal Current
IEEE 802.3af	44 V	2 pairs (CAT 3 or better)	15.4 W	12.95 W	350 mA
IEEE 802.3at	(44 to 57) V	2 pairs (CAT 5 or better)	30 W	25.5 W	600 mA

LLDP-MED (TIA-1057) with PoE+ (IEEE 802.3at)

The IEEE 802.1AB standard, Link Layer Discovery Protocol (LLDP) was designed to provide a multi-vendor solution for the discovery of network devices and accurate physical topology of how these devices are connected to one another. LLDP allows network devices to advertise their basic configuration and device capabilities to other network devices on the same LAN.

The IEEE 802.1AB standard was extended by the Telecommunications Industry Association (TIA) to fill the need for multi-vendor VoIP deployments. The TIA created the TIA-1057 standard, Link Layer Discovery Protocol Media Endpoint Devices (LLDP-MED), which allows for Media Endpoint Devices, such as VoIP phones, to exchange configuration information, including Power over Ethernet management. The TIA-1057 standard and the IEEE 802.3at standard provide for the following advanced PoE management capabilities:

- Fine grain PoE power allocation (1 watt granularity instead of wider power class bands)
- Power priority of the PD being supplied power
- Backup power conservation to extend UPS battery life

The IEEE 802.3at standard provides a capability for power re-negotiation with LLDP-MED.

PoE and PoE+ Applications

Products designed to the IEEE 802.3af (PoE) standard and IEEE 802.3at (PoE+) standard provide the benefits of lower installation costs, installation flexibility, and remote power monitoring and device management. Products supporting IEEE 802.3at can use higher power levels, along with dynamic power management when using LLDP-MED to exchange configuration data.

Power Device (PD) Discovery

The first step for PSE equipment is to determine whether a device plugged into a port is a valid Powered Device (PD). If it is, it will require power as well as network communication through the attached LAN cable.

The IEEE 802.3af-2003 and IEEE 802.3at-2009 standards for device detection involves applying a DC voltage between the transmit and receive wire pairs, and measuring the received current.

A PSE will expect to see approximately 25K Ohm resistance and 150nF capacitance between the transmit and receive wire pairs for the device to be considered a valid PD. A range around these values is specified in the IEEE 802.3af and IEEE 802.3at Power Ethernet standards.

The PSE will check for the presence of PDs on connected ports at regular intervals, so that power can be removed when a PD is no longer connected. Legacy (pre-IEEE 802.3af Power Ethernet standard) PDs are also detected by the PSE by default. See **"power-inline allow-legacy" on page 23.5**.

Power Classes

Once a PD is discovered, PSE initiates a PD classification test by applying a DC voltage to the port. If the PD supports optional power classification it will apply a load to the line to indicate to the PSE the classification the device requires.

Since PDs may require differing power ranges, the IEEE 802.3af and IEEE 802.3at Power Ethernet standards classifies PDs according to their power consumption. By providing the PSE with its power range, the PD allows the PSE to supply power with greater efficiency. The power classes as outlined by IEEE 802.3af and IEEE 802.3at are as follows showing the different PD classes and the PSE power output for each corresponding PD power range:

PD Class	Power Available at PD	Power Supplied from PSE
0	0.44 W to 12.95 W	15.4 W
1	0.44 W to 3.84 W	4.0 W
2	3.84 W to 6.49 W	7.0 W
3	6.49 W to 12.95 W	15.4 W
4	12.95 W to 25.5 W	30 W

Once the PSE has detected the PDs IEEE 802.3af or IEEE 802.3at power class, it can manage the power allocation by subtracting the PDs class maximum value from the overall power budget. This allows for control and management of power allocation when there is not enough power available from the PSE to supply maximum power to all ports. Any unclassified PD is considered to be a class 0 device.

To view the PD class that has been configured for each PoE port, apply the following command:

```
awplus# show power-inline
```

Typical Values for PD Power Consumption

The IEEE 802.3af standard specifies the delivery of up to 15.4 watts (W) per port to PoE devices. This enables a variety of possible devices to make use of the available power. The maximum power consumed by a PD, as specified by the IEEE 802.3af standard, is 12.95 W. The system provides the 'extra' power (up to 15.4 W) to compensate for losses in the cable. Some common PoE device power requirements are:

PoE Device	PoE Power Requirement
IP phone	3 W-6 W
Wireless access point	4 W-11 W
IP security camera	5 W-12 W

The IEEE 802.3at standard supports delivery of up to 30 W per port that may be used to deliver power to PoE+ devices. This allows a variety of possible devices to make use of the available power. The maximum power consumed by a PD, as specified by the IEEE 802.3at standard, is 25.5 W. The system provides the 'extra' power (up to 30 W) to compensate for line loss. Some common PoE+ device power requirements are:

PoE+ Device	PoE+ Power Requirement
Wireless Access Point (with LLDP-MED support)	12 W-24 W
Pan Tilt and Zoom powered IP security camera	12 W-24 W

Refer to the LLDP chapters **Chapter 69, LLDP, LLDP-MED and Voice VLAN Introduction and Configuration** and **Chapter 70, LLDP Commands** for information about power monitoring at the PD.

Power through the Cable

10/100BASE-TX Endpoint Mode

The IEEE 802.3af and IEEE 802.3at standards describe two methods for applying PoE over twisted pair cabling are termed “alternatives A and B”. Alternative A applies power to the data carrying cable pairs (using pins 1-2 and 3-6). Alternative B applies the power to the spare cable pairs (using pins 4-5 and 7-8).

The switch uses “alternative A” to apply power to its PDs. An IEEE compliant PD should be able to receive PoE using either of the two wiring methods.

1000BASE-T Endpoint Mode

An amendment to the IEEE 802.3at (2008) standard defines PoE cable connections for data transmission at 1 GHz. Although data is carried over all four cable pairs, the same cable pinning is used for PoE. i.e. alternative A applies power to the cable using pins 1-2 and 3-6, and alternative B applies the power to the cable using pins 4-5 and 7-8.

Cable Types

Although the IEEE standards 802.3af and 802.3at indicate minimum cable types for each standard version; using cables of a higher rating will reduce the cable resistance, allowing more power to be provided from the PSE to the PD. Also the power negotiation process that takes place between the PD and the PSE takes no account of the cable type that connects them, therefore the cabling used should be rated to meet the highest power that your PSE is able to supply.

A further factor is that network operation at 1 Gbps places higher demands on the cabling type used. These demands are increased when power is also carried over these cables.

For more information on twisted-pair cable selection for PoE, see the switch's **Installation Guide**.

Static and Automatic Power Allocation

When configuring PoE on your switch, you can either allow each port to auto-negotiate its power requirement, based on the power class of its connected PD, or you can statically allocate fixed power levels to each port.

Where dynamic PoE power assignment is used, the total power drawn from your switch's power supply will be the total of the individual power requirements of each port. See **"power-inline max" on page 23.8**

PoE and PoE+ Implementation

The following GS900MX/MPX series switches support PoE:

- GS924MPX
- GS948MPX

This section explains how to implement PoE on this switch.

Power Capacity

The following information is provided as a guide, and we recommend that you consult the appropriate Installation Guide for your particular switch for more detailed information.

PoE Port Allocation and Distribution

The total power available for PoE is dependent on the capacity of the power supply. How this power is distributed across the available PoE ports depends on the PoE configuration applied to the switch, particularly how you set the **power-inline priority** and **power-inline max** commands.

The AT-GS924MPX and AT-GS948MPX switches are both Layer 2 PoE+ Gigabit Ethernet switches with SFP and SFP+ support.

Power Threshold

The switch can be configured to send a Simple Network Management Protocol (SNMP) trap to your management workstation and records an entry in the event log whenever the total power requirements of the powered devices exceed the specified percentage of the total maximum power available on the switch. With the default setting of 80% applied, the switch sends an SNMP trap when the PoE devices require more than 80% of the maximum available power on the switch.

To adjust the threshold, use the command:

```
awplus(config)# power-inline usage-threshold <1-99>
```

For your management workstation to receive traps from your switches, you must configure SNMP on the switch by specifying the IP address of the workstation. The management workstation will also record an entry in the event log whenever power consumption of the switch has returned to a value that is less than the power limit threshold.

To set the SNMP traps (notifications) for PoE, use the command:

```
awplus(config)# snmp-server enable trap power-inline
```

See **Chapter 66, SNMP Introduction** for information about configuring SNMP traps for PoE. See **Chapter 67, SNMP Commands** for command examples to configure SNMP traps for PoE.

Negotiating Power Requirements

When configuring PoE on your switch, you can either allow each port to auto-negotiate its power requirement, based on the power class of its connected PD, or you can statically configure each port to have a fixed power allocation.

Where dynamic PoE power assignment is used, the total power assigned from your switch's power supply will be the total of the individual power requirements assigned to each port.

To enable your PoE ports to dynamically allocate their power, set the **"power-inline max" on page 23.8** to its default by entering, no power-inline max.

PoE Port Management

PoE is enabled by default on all non-SFP (or SFP+) RJ-45 ports. You can connect either a powered or non-powered device to a PoE-enabled port without having to re-configure the port. This is because PD detection is carried out before any power is supplied to the connected device.

PoE can be administratively enabled or disabled on each port using the **power-inline enable** command in Interface Configuration mode. To disable PoE on a selected port, use the command:

```
awplus(config-if)# no power-inline enable
```

Powered Device (PD) Detection

Your switch applies two methods to detect the connection of a PD. The first method applies the resistance and capacitance methods defined in the IEEE standards, see **"Power Device (PD) Discovery" on page 22.5**. The second method is applied to detect the connection of legacy PDs. This method involves measuring for a large capacitance value. The IEEE method is tried first, and if this fails to detect a PD, the second method is applied.

By default, legacy PD detection is enabled on all ports. To disable legacy PD detection, use the command:

```
awplus(config)# no power-inline allow-legacy
```

The switch applies its PD detection process in real time to all PoE enabled ports. It will not supply power to any PoE enabled port unless it detects the connection of a valid PD.

Port Prioritization

Port prioritization enables you to assign ports to be one of the following three priority levels:

- Critical
- High
- Low

Where the power required collectively by the Powered Devices (PDs) is greater than the PSUs are able to supply, these priority levels will be used to sequentially remove power from the PDs in an order of their importance.

Critical The highest priority level. Ports set to this level are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all the Critical ports are receiving power. Your most critical powered devices should be assigned to this level. If there is not enough power to support all the ports set to the Critical priority level, power is provided to the ports based on port number, in ascending order.

High The second highest level. Ports set to this level receive power only if all the ports set to the Critical level are already receiving power. If there is not enough power to support all of the ports set to the High priority level, power is provided to the ports based on port number, in ascending order.

Low The lowest priority level. This is the default setting. Ports set to this level only receive power if all the ports assigned to the other two levels are already receiving power. As with the other levels, if there is not enough power to support all of the ports set to the Low priority level, power is provided to the ports based on port number, in ascending order

If power needs to be removed from some of the PoE ports, where for example, one of the power supplies is disconnected; power will be removed from these ports in the order Low, High, and Critical. In addition, within each of these priority categories, lower numbered ports will be given higher priority than higher numbered ports; i.e. the lower the port number, the higher its PoE priority (within its particular category).

You can set the port priority by using the command:

```
awplus# power-inline priority
```

For more details on using this command see **"power-inline priority" on page 23.10**.

Note

Power allocation is dynamic. Ports supplying power may stop powering a PD if the switch's power capacity has reached maximum usage and new PD's are connected to ports with a higher priority, which become active.

To ensure continued operation of a PD if the power resources of the switch are exceeded you should install a PD to a lower numbered PoE port with the Critical priority level configured.

Software Monitoring

There are four PoE **show** commands available that return information about the PoE settings on your switch.

The **show power-inline** command displays the power threshold set, a power usage percentage, and power consumed by each switch port.

```
awplus# show power-inline
```

The **show power-inline counters** command displays PoE event counters from the PoE MIB (RFC 3621).

```
awplus# show power-inline counters
```

The **show power-inline interface** command displays a summary of all PoE information, including power limit, power consumed, and power class.

```
awplus# show power-inline interface
```

The **show power-inline interface detail** command displays all PoE information, including power limit, power consumed, and power class.

```
awplus# show power-inline interface detail
```

You can also specify an individual PoE port, a range of PoE ports, or a selection of PoE ports with the **show power-inline interface detail** command when using the <*port-list*> option, as shown below for a PoE port, a selection of PoE ports, and a range of PoE ports:

```
awplus# show power-inline interface port1.0.2 detail

awplus# show power-inline interface port1.0.2,port1.0.4
        detail

awplus# show power-inline interface port1.0.2-port1.0.4
        detail
```

PoE and PoE+ Configuration

This section is based around PoE configuration tasks for the Allied Telesis AT-GS924MPX and AT-GS948MPX switches running the AlliedWare Plus™ Operating System.

Add a Description for a PoE or PoE+ Port

You can add a description (typically the device type) for a PoE port, which the switch will display in certain Show commands. Knowing the type of PD is useful when inspecting PD Class power usage. The description entered will appear in the following commands under Device, or Powered Device Type, for each PoE or PoE+ port:

show power-inline interface command on page 23.20 and,

show power-inline interface detail command on page 23.22.

In the following example a description is added for the PoE port listed as **port1.0.2** to display the words "**Desk Phone"** in the show output of the commands mentioned above.

Command	Description
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `configure interface port1.0.2`	Specify the PoE or PoE+ port to be configured and enter Interface mode.
`awplus(config-if)#` `power-inline description Wireless Access Point # 1`	The description "Desk Phone" will be displayed in all PoE show command output for `port1.0.2`.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show power-inline interface port1.0.2`	Display the PoE status for `port1.0.2` to confirm that your PoE configuration on the PSE has been successful. If a PD is connected to the configured PoE port then power consumption as well as power allocation values will display.
`awplus#` `copy running-config startup-config`	Save your running-config to the startup-config to keep your PoE configuration after a switch restart or reboot.

Configuring Capacity and Priority on a PoE or PoE+ Port

The following commands set a higher priority and a lower maximum power for a PoE or PoE+ port. This prevents high powered PDs from being connected to a PoE or PoE+ port reserved for low powered PDs. Follow the configuration table below to configure **port1.0.2**.

Command	Description
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `configure interface port1.0.2`	Specify the PoE or PoE+ port to be configured and enter Interface mode.
`awplus(config-if)#` `power-inline priority high`	Specify a higher priority for the PoE or PoE+ port than the default low setting.
`awplus(config-if)#` `power-inline max 4000`	Specify the lowest available power that the PSE can supply to the PD: 4000 mW.
`awplus(config-if)#` `exit`	Return to Global Configuration mode.
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show power-inline interface port1.0.2`	Display the PoE status for `port1.0.2` to confirm that your PoE configuration on the PSE has been successful. If a PD is connected to the configured PoE port then power consumption as well as power allocation values will display.
`awplus#` `copy running-config startup-config`	Save your running-config to the startup-config to keep your PoE configuration after a switch restart or reboot.

Remotely Monitoring Power for all Connected PDs

By using the **power-inline usage-threshold** command and the **snmp-server enable trap** commands together you can remotely monitor PD power requests on the PSE.

Note that you will need to configure SNMP first for this. For more information on configuring SNMP, see the following chapters in your switch's software reference:

- **Chapter 66, SNMP Introduction**
- **Chapter 67, SNMP Commands**
- **Chapter 68, SNMP MIBs**

For example, if the PD is a Class 0 (default class) or a Class 3 (15400 mW) PD then the PSE budgets 15400 mW for the PD regardless of the actual amount of power needed by the PD.

The following procedure allows you to remotely monitor power usage for all connected PDs. Follow the configuration table to configure the PSE.

Command	Description
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `service power-inline`	Enable PoE globally for the PSE. This will also enable PoE globally for all PoE ports on all connected stacked switches.
`awplus(config)#` `snmp-server enable trap power-inline`	Configure SNMP notification so an SNMP trap is sent when the power usage threshold is exceeded to trigger an alarm.
`awplus(config)#` `power-inline usage-threshold 75`	Specify SNMP notifications are generated when the power supplied exceeds 75% of the nominal PSE power available.
`awplus(config)#` `exit`	Return to Privileged Exec mode.
`awplus#` `show power-inline`	Display the PoE status for all PoE ports on the PSE. The PD Class, power consumption, and power allocated per PoE port displays for all PoE ports on the PSE.
`awplus#` `copy running-config startup-config`	Save your running-config to the startup-config to keep your PoE configuration after a switch restart or reboot.

Chapter 23: Power over Ethernet Commands

Introduction 23.2
Command List 23.2
clear power-inline counters interface 23.3
debug power-inline 23.4
power-inline allow-legacy 23.5
power-inline description 23.6
power-inline enable 23.7
power-inline max 23.8
power-inline priority 23.10
power-inline usage-threshold 23.12
service power-inline 23.13
show debugging power-inline 23.14
show power-inline 23.15
show power-inline counters 23.18
show power-inline interface 23.20
show power-inline interface detail 23.22

Introduction

Power over Ethernet (PoE) is a technology allowing devices such as IP phones to receive power over existing LAN cabling.

PoE is configured using the commands in this chapter. Note the Power Sourcing Equipment (PSE) referred to throughout this chapter is an Allied Telesis PoE switch running the AlliedWare Plus™ Operating System, supporting the IEEE 802.3af and IEEE 802.3at Power Ethernet standards. The Powered Device (PD) referred to throughout this chapter is a PoE or PoE+ powered device, such as an IP phone or a Wireless Access Point (WAP).

The commands in this chapter are available on the Allied Telesis AT-GS924MPX and AT-GS948MPX switches. These switches are Layer 2 PoE+ Gigabit Ethernet switches with SFP and SFP+ support.

Command List

This chapter contains an alphabetical list of commands used to configure Power over Ethernet (PoE). Each command contains a functional description and shows examples of configuration and output screens for show commands. These commands are only supported on PoE capable ports. An error message will display on the console if you enter a PoE command on a port that does not support PoE. The following chapters offer further information for configuring PoE on Allied Telesis switches.

- **Chapter 22, Power over Ethernet Introduction** for introductory information about PoE and how to configure PoE on Allied Telesis switches.
- **Chapter 68, SNMP MIBs** for information about which PoE MIB objects are supported.
- **Chapter 66, SNMP Introduction** for information about SNMP traps.
- **Chapter 67, SNMP Commands** for SNMP command descriptions used when configuring SNMP traps for PoE.

clear power-inline counters interface

This command will clear the counters from a specified port, a range of ports, or all ports on the Power Sourcing Equipment (PSE). If no ports are entered then PoE counters for all ports are cleared. It will also clear all Power over Ethernet (PoE) counters supported by the Power Ethernet MIB (RFC 3621).

Syntax `clear power-inline counters interface [<port-list>]`

Parameter	Description
<port-list>	Selects the port or ports whose counters are to be cleared.

Mode Privileged Exec

Usage The PoE counters are displayed with the **show power-inline counters** command.

Examples To clear the PoE counters for `port1.0.2` only, use the following command:

```
awplus# clear power-inline counters interface port1.0.2
```

To clear the PoE counters for `port1.0.1` through `port1.0.10`, use the following command:

```
awplus# clear power-inline counters interface port1.0.1-
port1.0.10
```

To clear the PoE counters for all ports, use the following command:

```
awplus# clear power-inline counters interface
```

Validation Commands **show power-inline counters**

debug power-inline

This command enables debugging display for messages that are specific to Power over Ethernet (PoE).

Use the **no** variant of this command to disable the specified PoE debugging messages.

Syntax

```
debug power-inline [all|event|info|power]
no debug power-inline [all|event|info|power]
```

Parameter	Description
`all`	Displays all (`event`, `info`, `nsm`, `power`) debug messages.
`event`	Displays event debug information, showing any error conditions that may occur during PoE operation.
`info`	Displays informational level debug information, showing high-level essential debugging, such as information about message types.
`power`	Displays power management debug information.

Default No debug messages are enabled by default.

Mode Privileged Exec

Usage Use the **terminal monitor** command to display PoE debug messages on the console.

Use the **show debugging power-inline** command to show the PoE debug configuration.

Examples To enable PoE debugging and start the display of PoE `event` and `info` debug messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline event info
```

To enable PoE debugging and start the display of all PoE debugging messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline all
```

To disable PoE debugging and stop the display of PoE `event` and `info` debug messages on the console, use the following command:

```
awplus# no debug power-inline event info
```

To disable all PoE debugging and stop the display of any PoE debugging messages on the console, use the following command:

```
awplus# no debug power-inline all
```

Validation Commands **show debugging power-inline**

Related Commands **terminal monitor**

power-inline allow-legacy

This command enables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

The no variant of this command disables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

Syntax

```
power-inline allow-legacy
no power-inline allow-legacy
```

Default Detection of legacy PDs is enabled on all ports on the Power Sourcing Equipment (PSE).

Mode Global Configuration

Examples To disable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline allow-legacy
```

To enable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# power-inline allow-legacy
```

Validation Commands **show power-inline**
show running-config power-inline

power-inline description

This command adds a description for a Powered Device (PD) connected to a PoE port.

The **no** variant of this command clears a previously entered description for a connected PD, resetting the PD description to the default (null).

Syntax

```
power-inline description <pd-description>
no power-inline description
```

Parameter	Description
<pd-description>	Description of the PD connected to the PoE capable port (with a maximum 256 character string limit per PD description).

Default No description for a connected PD is set by default.

Mode Interface Configuration

Usage Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding **interface (to configure)** command. If you specify a range or list of ports they must all be PoE capable ports.

Examples To add the description `Desk Phone` for a connected PD on `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline description Desk Phone
```

To clear the description as added above for the connected PD on `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline description
```

Validation Commands **show power-inline interface**
show running-config power-inline

power-inline enable

This command enables Power over Ethernet (PoE) to detect a connected Powered Device (PD) and supply power from the Power Sourcing Equipment (PSE).

The **no** variant of this command disables PoE functionality on the selected PoE port(s). No power is supplied to a connected PD after PoE is disabled on the selected PoE port(s).

Syntax

```
power-inline enable
no power-inline enable
```

Default PoE is enabled by default on all ports on the PSE.

Mode Interface Configuration

Usage In a stack of switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports from the preceding **interface (to configure)** command. If you specify a range or list of ports they must all be PoE capable ports.

No PoE log messages are generated for specified PoE port(s) after PoE is disabled. The disabled PoE port(s) still provide Ethernet connectivity after PoE is disabled.

Examples To disable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no power-inline enable
```

To enable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# power-inline enable
```

Validation Commands

show power-inline
show power-inline interface
show power-inline interface detail
show running-config power-inline

power-inline max

This command sets the "maximum" power allocated to a Power over an Ethernet (PoE and PoE+) port. The amount of power actually supplied to the port depends on the power requirements of the connected PD. It is also a function of the total PoE power loading on the switch and the PoE priority set for the port by the **power-inline priority** command. However this command (power-inline max) does apply a "maximum" value to the power that the port is able to supply.

Note that the value set by this command will be the figure the switch will use when apportioning the power budget for its ports. For example, if 15.4 W is assigned to a port whose PD only consumes 5 W, the switch will reserve the full 15.4 W for this port when determining its total power PoE power requirement.

Note that the value set by this command will be the figure the switch will use when apportioning the power budget for its ports. For example, if 15.4 W is assigned to a port whose PD only consumes 5 W, the switch will reserve the full 15.4 W for this port when determining its total power PoE power requirement.

The **no** variant of this command sets the maximum power supplied to a PoE port to the default, which is set to the maximum power limit for the class of the connected Powered Device (PD).

Syntax

```
power-inline max <4000-30000>

no power-inline max
```

Parameter	Description
<4000-30000>	The maximum power allocated to a PoE port in milliwatts (mW).

Default The Power Sourcing Equipment (PSE) supplies the maximum power limit for the class of the PD connected to the port by default.

Power limits for all classes of PDs are listed in **"Power Classes" on page 22.6**. See **Chapter 22, Power over Ethernet Introduction** for further PoE information.

Mode Interface Configuration

Usage In a stack of switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding **interface (to configure)** command. If you specify a range or list of ports they must all be PoE capable ports.

If you select a range of PoE ports in Interface Configuration mode before issuing this command, then each port in the range selected will have the same maximum power value configured. If the PoE port attempts to draw more than the maximum power, this is logged and all power is removed. Note that the value entered is rounded up to the next value supported by the hardware.

See the actual value used, as shown after command entry, in the sample console output below:

```
awplus#configure terminal
awplus(config)#interface port1.0.1
awplus(config-if)#power-line max 5300
% The maximum power has been rounded to 5450mW in hardware.
```

Refer to **Chapter 69, LLDP, LLDP-MED and Voice VLAN Introduction and Configuration** and **Chapter 70, LLDP Commands** for information about power monitoring at the PD.

Note the difference in power supplied from the PSE to the power available at the PD due to line loss.

The **"Power Classes" on page 22.6** shows the difference between the power supplied from the PSE and the power available at the PD.

Examples

To set the maximum power supplied to ports in the range `1.0.2 to 1.0.4` to 6450mW per port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# power-inline max 6450
```

To set the maximum power supplied to `port1.0.2`, to `6450` mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline max 6450
```

To clear the user-configured maximum power supplied to `port1.0.2`, and revert to using the default maximum power of 30000 mW, use the following commands:

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

Validation Commands

show power-inline interface
show running-config power-inline

power-inline priority

This command sets the Power over Ethernet (PoE) priority level of a PoE port to one of three available priority levels:

- low
- high
- critical

The **no** variant of this command restores the PoE port priority to the default (low).

Syntax

```
power-inline priority {low|high|critical}

no power-inline priority
```

Parameter	Description
`low`	The lowest priority for a PoE enabled port (default). PoE ports set to `low` only receive power if all the PoE ports assigned to the other two levels are already receiving power.
`high`	The second highest priority for a PoE enabled port. PoE ports set to `high` receive power only if all the ports set to `critical` are already receiving power.
`critical`	The highest priority for a PoE enabled port. PoE ports set to `critical` are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all Critical ports are receiving power.

Default The default priority is `low` for all PoE ports on the Power Sourcing Equipment (PSE).

Mode Interface Configuration

Usage This command is supported on all PoE capable ports, whether operating as a stand-alone switch, or within a VCStack.

Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding **interface (to configure)** command. If you specify a range or list of ports they must all be PoE capable ports.

PoE ports with higher priorities are given power before PoE ports with lower priorities. If the priorities for two PoE ports are the same then the lower numbered PoE port is given power before the higher numbered PoE port.

See **"Port Prioritization" on page 22.10** for further information about PoE priority.

Examples To set the priority level to `high` for `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline priority high
```

To reset the priority level to the default for `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline priority
```

Validation Commands
show power-inline
show power-inline interface
show running-config power-inline

Related Commands **power-inline usage-threshold**

power-inline usage-threshold

This command sets the level at which the Power Sourcing Equipment (PSE) will issue a message that the power supplied to all Powered Devices (PDs) has reached a critical level of the nominal power rating for the PSE. The level is set as a percentage of total available power.

The **no** variant of this command resets the notification usage-threshold to the default (80% of the nominal power rating of the PSE).

Syntax

```
power-inline usage-threshold <1-99>

no power-inline usage-threshold
```

Parameter	Description
<1-99>	The usage-threshold percentage configured with this command.

Default The default power usage threshold is 80% of the nominal power rating of the PSE.

Mode Global Configuration

Usage Use the **snmp-server enable trap** command on page 67.18 to configure SNMP notification. An SNMP notification is sent when the usage-threshold, as configured in the example, is exceeded.

Examples To generate SNMP notifications when power supplied exceeds 70% of the nominal PSE power, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
awplus(config)# power-inline usage-threshold 70
```

To reset the notification threshold to the default (80% of the nominal PSE power rating), use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

Validation Commands **show power-inline interface**
show running-config power-inline

Related Commands **snmp-server enable trap**

service power-inline

This command enables Power over Ethernet (PoE) globally on the Power Sourcing Equipment (PSE) for all PoE ports.

Syntax

```
service power-inline
no service power-inline
```

Default PoE functionality is enabled by default on the PSE.

Mode Global Configuration

Usage In a stack, issuing this command enables PoE globally for all PoE ports.

In a stack configuration, only stack members containing PoE hardware will have PoE enabled by default in software.

Examples To disable PoE on the PSE, use the following commands:

```
awplus# configure terminal
awplus(config)# no service power-inline
```

To re-enable PoE on the PSE, if PoE has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service power-inline
```

Validation Commands **show power-inline**
show running-config power-inline

show debugging power-inline

This command displays Power over Ethernet (PoE) debug settings.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging power-inline`

Mode User Exec and Privileged Exec

Example To display PoE debug settings, use the following command:

```
awplus# show debugging power-inline
```

Output **Figure 23-1: Example output from the show debugging power-inline command**

```
awplus#show debugging power-inline
PoE Debugging status:
PoE Informational debugging is disabled
PoE Event debugging is disabled
PoE Power Management debugging is disabled
PoE NSM debugging is enabled
```

Related Commands **debug power-inline**
terminal monitor

show power-inline

This command displays the Power over Ethernet (PoE) status for all ports on the Power Sourcing Equipment (PSE).

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show power-inline`

Mode User Exec and Privileged Exec

Example To display the PoE status for all ports on the PSE, use the following command:

```
awplus# show power-inline
```

Output **Figure 23-2: Example output from the show power-inline command**

```
awplus#show power-inline
PoE Status:

Stack Member 2
 Nominal Power: 370W
 Power Allocated: 246W
 Actual Power Consumption: 151W
 Operational Status: On
 Power Usage Threshold: 80% (296W)

PoE Interface:
Interface  Admin   Pri  Oper    Power   Device    Class  Max(mW)
port2.0.1  Enabled Low  Powered  3840   n/a          1    4000 [C]
port2.0.2  Enabled High Powered  6720   n/a          2    7000 [C]
port2.0.3  Enabled Low  Powered 14784   n/a          3   15400 [C]
port2.0.4  Enabled Crit Powered 14784   n/a          3   15400 [C]
port2.0.5  Enabled Crit Powered  3840   n/a          1    4000 [C]
port2.0.6  Enabled High Powered  6720   n/a          2    7000 [C]
port2.0.7  Enabled Low  Powered 14784   n/a          3   15400 [C]
```

Table 23-1: Parameters in the show power-inline command output

Parameter	Description
`Nominal Power`	The nominal power available on the switch in watts (W).
`Power Allocated`	The current power allocated in watts (W) that is available to be drawn by any connected Powered Devices (PDs). This is updated every 5 seconds.
`Actual Power Consumption`	The current power consumption in watts (W) drawn by all connected Powered Devices (PDs). This is updated every 5 seconds.
`Operational Status`	The operational status of the PSU hardware on the PSE when this command was issued: ■ **On** if the PSU as installed inside the PSE is switched on. ■ **Off** when the PSU in the PSE is switched off (an RPS may be connected to the PSE to power PoE instead of the PSU). ■ **Fault** when there is an issue with the PSE PSU hardware.
`Power Usage Threshold (%)`	The configured SNMP trap / log threshold for the PSE, as configured from a **power-inline usage-threshold** command.
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Admin`	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.
`Pri`	The current PoE priorities for PoE ports on the PSE, as configured from a **power-inline priority** command: ■ **Low** displays when the `low` parameter is issued. The lowest priority for a PoE enabled port (default). ■ **High** displays when the `high` parameter is issued. The second highest priority for a PoE enabled port. ■ **Crit** displays when the `critical` parameter is issued. The highest priority for a PoE enabled port.
`Oper`	The current PSE PoE port state when this command was issued: ■ **Powered** displays when there is a PD connected and power is being supplied from the PSE. ■ **Disabled** displays when supplying power would make the PSE go over the power budget. ■ **Off** displays when PoE has been disabled for the PoE port. **Fault** displays when a PSE goes over its power allocation.
`Power`	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
`Device`	The description of the connected PD device if a description has been added with the **power-inline description** command. No description is shown for PDs not configured with the **power-inline description** command.

Table 23-1: Parameters in the show power-inline command output (cont.)

Parameter	Description
`Class`	The class of the connected PD, if power is being supplied to the PD from the PSE. See the **Power over Ethernet Introduction** chapter for further information about PD classes and the power levels assigned per class.
`Max (mW)`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: ■ **[U]** if the power limit for a port was user configured (with the **power-inline max** command). ■ **[L]** if the power limit for a port was supplied by LLDP. ■ **[C]** if the power limit for a port was supplied by the PD class.

Related Commands

show power-inline counters
show power-inline interface

show power-inline counters

This command displays Power over Ethernet (PoE) event counters for ports on the Power Sourcing Equipment (PSE). The PoE event counters displayed can also be accessed by objects in the PoE MIB (RFC 3621). See **Chapter 68, SNMP MIBs** for information about which PoE MIB objects are supported.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show power-inline counters [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display all PoE event counters for them.

Mode User Exec and Privileged Exec

Usage To display all PoE event counters for all PoE ports on the PSE, do not enter the optional interface parameter.

Examples To display all PoE event counters for all PoE ports on the PSE, use the command:

```
awplus# show power-inline counters
```

To display the PoE event counters for the port range `1.0.1` to `1.0.3`, use the command:

```
awplus# show power-inline counters interface port1.0.1-1.0.3
```

Output **Figure 23-3: Example output from the show power-inline counters command**

```
awplus#show power-inline counters interface port1.0.4-port1.0.12
PoE Counters:
Interface   MPSAbsent Overload Short Invalid Denied
port1.0.4   0         0        0     0       0
port1.0.5   0         0        0     0       0
port1.0.6   0         0        0     0       0
port1.0.7   0         0        0     0       0
port1.0.8   0         0        0     0       0
port1.0.9   0         0        0     0       0
port1.0.10  0         0        0     0       0
port1.0.11  0         0        0     0       0
port1.0.12  0         0        0     0       0
```

Table 23-2: Parameters in the show power-inline counters command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`MPSAbsent`	The number of instances when the PoE MPS (Maintain Power Signature) signal has been lost. The PoE MPS signal is lost when a PD is disconnected from the PSE. Also increments `pethPsePortMPSAbsentCounter` in the PoE MIB.
`Overload`	The number of instances when a PD exceeds its configured power limit (as configured by the **power-inline max** command). Also increments `pethPsePortOverLoadCounter` in the PoE MIB.
`Short`	The number of short circuits that have happened with a PD. Also increments `pethPsePortShortCounter` in the PoE MIB.
`Invalid`	The number of times a PD with an Invalid Signature (where the PD has an open or short circuit, or is a legacy PD) is detected. Also increments `pethPseInvalidSignatureCounter` in the PoE MIB.
`Denied`	The number of times a PD has been refused power due to power budget limitations for the PSE. Also increments `pethPsePortPowerDeniedCounter` in the PoE MIB.

Related Commands

clear power-inline counters interface
show power-inline
show power-inline interface

show power-inline interface

This command displays a summary of Power over Ethernet (PoE) information for specified ports. If no ports are specified then PoE information is displayed for all ports on the Power Sourcing Equipment (PSE).

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show power-inline interface [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display PoE specific information in the show output.

Mode User Exec and Privileged Exec

Usage To display PoE information for all PoE ports on the PSE, do not specify any ports.

Example To display the PoE port specific information for all PoE ports on the switch, use the following command:

```
awplus# show power-inline interface
```

To display the PoE port specific information for the port range `1.0.1` to `1.0.4`, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.4
```

Output **Figure 23-4: Example output from the show power-inline interface command**

```
awplus#show power-inline interface port1.0.1-port1.0.4
Interface  Admin    Pri  Oper     Power Device      Class Max(mW)
port1.0.1  Disabled Low  Disabled     0 n/a         n/a   n/a
port1.0.2  Enabled  High Powered   3840 Desk Phone  1     5000 [U]
port1.0.3  Enabled  Crit Powered   6720 AccessPoint 2     7000 [C]
port1.0.4  Disabled Low  Disabled     0 n/a         n/a   n/a
```

Table 23-3: Parameters in the show power-inline interface command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Admin`	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.
`Pri`	The current PoE priorities for PoE ports on the PSE, as configured from a **power-inline priority** command: ■ **Low** displays when the `low` parameter is issued. The lowest priority for a PoE enabled port (default). ■ **High** displays when the `high` parameter is issued. The second highest priority for a PoE enabled port. ■ **Crit** displays when the `critical` parameter is issued. The highest priority for a PoE enabled port.
`Oper`	The current PSE PoE port state when this command was issued: ■ **Powered** displays when there is a PD connected and power is being supplied from the PSE. ■ **Denied** displays when supplying power would make the PSE go over the power budget. ■ **Disabled** displays when the PoE port is administratively disabled. ■ **Off** displays when PoE has been disabled for the port. ■ **Fault** displays when a PSE goes over its power allocation.
`Power`	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
`Device`	The description of the connected PD device if a description has been added with the **power-inline description** command. No description is shown for PDs not configured with the **power-inline description** command.
`Class`	The class of the connected PD, if power is being supplied to the PD from the PSE. See **"Power Classes" on page 22.6** in **Chapter 22, Power over Ethernet Introduction** for further information about PD classes and the power assigned per class.
`Max (mW)`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: ■ **[U]** if the power limit for a port was user configured (with the **power-inline max** command). ■ **[L]** if the power limit for a port was supplied by LLDP. ■ **[C]** if the power limit for a port was supplied by the PD class.

Related Commands

show power-inline
show power-inline interface detail

show power-inline interface detail

This command displays detailed information for specified Power over Ethernet (PoE) port(s) on the Power Sourcing Equipment (PSE).

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show power-inline interface [<port-list>] detail`

Parameter	Description
<port-list>	Enter the PoE port(s) to display the PoE port specific information.

Mode User Exec and Privileged Exec

Usage To show detailed PoE information for all ports on the PSE, do not specify any ports.

The power allocated to each port is listed in the `Power allocated` row, and is limited by the maximum power per Powered Device (PD) class, or a user configured power limit.

Example To display detailed PoE port specific information for the port range `1.0.1` to `1.0.2`, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.2
       detail
```

Output **Figure 23-5: Example output from the show power-inline interface detail command**

```
awplus#show power-inline interface port1.0.1-1.0.2 detail
Interface port1.0.1
  Powered device type: Desk Phone #1
  PoE admin enabled
  Priority Low
  Detection status: Powered
  Current power consumption: 4800 mW
  Powered device class: 1
  Power allocated: 5000 mW (from configuration)
  Detection of legacy devices is disabled
  Powered pairs: Data
Interface port1.0.2
  Powered device type: Access Point #3
  PoE admin enabled
  Priority High
  Detection status: Powered
  Current power consumption: 6720 mW
  Powered device class: 2
  Power allocated: 7000 mW (from powered device class)
  Detection of legacy devices is enabled
  Powered pairs: Data
```

Table 23-4: Parameters in show power-inline interface detail command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Powered device type:`	The name of the PD, if connected and if power is being supplied to the PD from the PSE, configured with the **power-inline description** command. **n/a** displays if a description has not been configured for the PD.
`PoE admin`	The administrative state of PoE on a PoE capable port, either **Enabled** or **Disabled** as configured from the **power-inline enable** command or the **no power-inline enable** command respectively.
`Priority`	The PoE priority of a port, which is either **Low,** or **High,** or **Critical**, as configured by the **power-inline priority** command.
`Detection status:`	The current PSE PoE port state when this command was issued: ■ **Powered** displays when there is a PD connected and power is being supplied from the PSE. ■ **Denied** displays when supplying power would make the PSE go over the power budget. ■ **Disabled** displays when the PoE port is administratively disabled. ■ **Off** displays when PoE has been disabled for the port. ■ **Fault** displays when a PSE goes over its power allocation.
`Current power consumption:`	The power consumption for the PoE port when this command was entered. Note that the power consumption may have changed since the command was entered and the power is displayed.
`Powered device class:`	The class of the connected PD if connected, and if power is being supplied to the PD from the PSE. See **Chapter 22, Power over Ethernet Introduction** chapter for further information about PD classes and the power assigned per class.
`Power allocated:`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: ■ **[U]** if the power limit for a port was user configured (with the **power-inline max** command). ■ **[L]** if the power limit for a port was supplied by LLDP. ■ **[C]** if the power limit for a port was supplied by the PD class.
`Detection of legacy devices is`	`[Enabled|Disabled]` The status of legacy PoE detection on the PoE port, as configured for the PoE port with the **power-inline allow-legacy** command.
`Powered pairs:`	`[Data|Spare]` The IEEE 802.3af and IEEE 802.3at standards allow for either **data** or **spare** twisted pairs to be used to transfer power to a PD. The powered pairs status for each port. AlliedWare Plus™ PoE switches implement IEEE 802.3af and IEEE 802.3at Endpoint PSE Alternative A (**Data**).

Related Commands

show power-inline
show power-inline interface

Part 3: IP and IPv6

- Chapter 24 Internet Protocol (IP) Addressing and Protocols
- Chapter 25 IP Addressing and Protocol Commands
- Chapter 26 IPv6 Introduction
- Chapter 27 IPv6 Commands
- Chapter 28 Route Selection
- Chapter 29 Routing Commands
- Chapter 30 RIP Configuration
- Chapter 31 RIP Commands

Chapter 24: Internet Protocol (IP) Addressing and Protocols

Introduction 24.2
Address Resolution Protocol (ARP) 24.3
- Static ARP Entries 24.3
- Timing Out ARP Entries 24.3
- Deleting ARP Entries 24.4
- ARP Logging 24.5

DNS Client 24.6
Internet Control Message Protocol (ICMP) 24.8
Checking IP Connections 24.9
- Ping 24.9
- Traceroute 24.9

Introduction

This chapter describes how to configure IPv4 addressing and the protocols used to help IP function on your network.

As well as the familiar Internet (with uppercase "I"), the term internet (with lowercase "i") can refer to any network (usually a wide area network) that uses the Internet Protocol. This chapter concentrates on this definition—a generalized network that uses IP as its network protocol.

Assigning an IP Address

To configure your device to perform IP routing (for example, to access the Internet) you need to configure IP. You also need to configure IP if you want to manage your device from any IP-based management process (such as SSH, Telnet, or SNMP).

Add an IP address to each of the interfaces that you want to process IP traffic.

You can configure an interface on your device with a static IP address, or with a dynamic IP address assigned using your device's DHCP client.

Static IP addresses

To add a static IP address to an interface, enter interface mode for the interface that you want to configure, then use the command:

```
awplus(config-if)# ip address <ip-addr/prefix-length>
                   [secondary] [label <label>]
```

where `<ip-address/m>` the IP address followed by a slash then the prefix length. Note that you cannot specify the mask in dotted decimal notation in this command.

For example, to give the interface vlan1 an address of 192.168.10.10, with a class C subnet mask, use the command:

```
awplus(config-if)# ip address 192.168.10.10/24
```

The **secondary** parameter allows you to add multiple IP addresses to an interface using this command. Each interface must have a primary IP address before you can add a secondary address. Your device treats secondary addresses the same as primary addresses in most instances, such as responding for ARP requests for the IP address. However, the only packets generated that have a secondary address as source address are routing updates. You can define up to 32 secondary addresses on a single interface.

DHCP dynamic addresses

When you use the DHCP client, it obtains the IP address and subnet mask for the interface, and other IP configuration parameters, from a DHCP server. To configure an interface to gain its IP configuration using the DHCP client, use the command:

```
awplus(config-if)# ip address dhcp [client-id <interface>]
                   [hostname <hostname>]
```

If an IP interface is configured to get its IP address and subnet mask from DHCP, the interface does not take part in IP routing until the IP address and subnet mask have been set by DHCP.

If you need to make a static entry in your DHCP server for the device, you need your device's MAC address, which you can display by using the command:

```
awplus# show interface
```

See **Chapter 64, Dynamic Host Configuration Protocol (DHCP) Introduction** for more information about DHCP.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is used by your device to dynamically learn the Layer 2 address of devices in its networks. Most hosts also have a MAC physical address in addition to the assigned IP address. For Ethernet, this is a 6-byte, globally unique number. ARP enables your device to learn the physical address of the host that has a given IP address.

When your device needs to forward packets to a destination that it does not know the Layer 2 address of, it broadcasts an ARP request to determine where to send the packet. The ARP request is a broadcast packet and includes the target IP address. All stations on the LAN receive this broadcast but only one host recognizes its own IP address. It replies, thereby giving your device its physical address.

Your device creates a dynamic ARP entry in its ARP cache, to record the IP address to physical address mapping (also called a binding). It uses that ARP entry to forward further packets to that address.

The ARP protocol is described in RFC 826, ***An Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware***.

Static ARP Entries

If your LAN includes hosts that do not support ARP, you can add a static ARP entry to the cache. However, it is rarely necessary to add an ARP entry this way. To add a static ARP entry, use the command:

```
awplus(config)# arp <ip-addr> <mac-address> [<port-number>]
                [alias]
```

Timing Out ARP Entries

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. If your device stops receiving traffic for a device specified in a dynamic ARP entry, it deletes the ARP entry after a configurable timeout period. Static ARP entries are not aged or automatically deleted.

Increasing the ARP timeout reduces the amount of network traffic. Decreasing the timeout makes your device more responsive to changes in network topology.

To set a timeout period, enter the interface mode, then use the command:

```
awplus(config-if)# arp-aging-timeout <0-432000>
```

Deleting ARP Entries

To remove a static ARP entry, use the command:

```
awplus(config)# no arp <ip-addr>
```

To clear the ARP cache of dynamic entries, use the command:

```
awplus# clear arp-cache
```

This removes the dynamic ARP entries for all interfaces.

To display the entries in the ARP cache, use the command:

```
awplus)# show arp
```

The ARP cache will be repopulated by the normal ARP learning mechanism. As long as the entries are relearned quickly enough, deleting dynamic ARP entries does not affect:

- routes
- the TCP/UDP connection status

ARP Logging

You can enable your device to log static and dynamic ARP entries, and you can select either default hexadecimal notation (HHHH.HHHH.HHHH) or standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) for the MAC addresses displayed in the ARP log output.

If this feature is enabled, ARP log messages are stored on the device in RAM. If the device is rebooted the ARP log messages are lost. ARP logging is disabled by default.

To enable ARP logging, use the command:

```
awplus(config)# arp log [mac-address-format ieee]
```

You can specify whether the MAC address is displayed in the default hexadecimal notation HHHH.HHHH.HHHH or in the standard IEEE format HH-HH-HH-HH-HH-HH.

To disable ARP logging, use the command:

```
awplus(config)# no arp log [mac-address-format ieee]
```

To display the ARP log messages, use the command:

```
awplus(config)# show log | include ARP_LOG
```

See the sample ARP log output and descriptions of the fields displayed in the sample ARP log output in the **arp log** command on page 25.6.

DNS Client

Your AlliedWare Plus™ device has a DNS Client that is enabled automatically when you add a DNS server to your device. This client allows you to use domain names instead of IP addresses when using commands on your device.

To add a DNS server to the list of servers that the device sends DNS queries to, use the command:

```
awplus(config)# ip name-server <ip-addr>
```

To check the list of servers that the device sends DNS queries to, use the command:

```
awplus# show ip name-server
```

To add a default domain name used to append to DNS requests, use the command:

```
awplus(config)# ip domain-name <domain-name>
```

For example, to use DNS to match hostnames to your internal network “example.net”, use the command:

```
awplus(config)# ip domain-name example.net
```

If you then use the command **ping host2**, your device sends a DNS request for host2.example.net. To check the domain name configured with this command, use the command:

```
awplus# show ip domain-name
```

Alternatively you can create a list of domain names that your device will try in turn by using the command:

```
awplus(config)# ip domain-list <domain-name>
```

For example, to use DNS to match incomplete hostnames to the top level domains “.com”, and “.net”, use the commands:

```
awplus(config)# ip domain-list .com
awplus(config)# ip domain-list .net
```

If you then use the command **ping alliedtelesis**, your device sends a DNS request for alliedtelesis.com and if no match was found your device would then try alliedtelesis.net. To check the entries in the domain list, use the command:

```
awplus# show ip domain-list
```

To disable the DNS client on your device, use the command:

```
awplus(config)# no ip domain-lookup
```

To check the status of the DNS Client on your device, and the configured servers and domain names, use the command:

```
awplus# show hosts
```

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) allows networking devices to send information and control messages to other devices or hosts. Your device implements all non-obsolete ICMP functions.

The following table lists the ICMP messages implemented by your device.

ICMP Message Type	Device Response
Echo reply (0)	This is used to implement the ping command. Your device sends out an echo reply in response to an echo request.
Destination unreachable (3)	This message is sent when your device drops a packet because it did not have a route to the destination.
Redirect (5)	Your device issues this message to inform a local host that its target is located on the same LAN (no routing is required) or when it detects a host using a non-optimal route (usually because a link has failed or changed its status). For example, if your device receives a packet destined to its own MAC address, but with a destination IP address of another host in the local subnet, it returns an ICMP redirect to the originating host. ICMP redirects are disabled on interfaces on which local proxy ARP is enabled.
Echo request (8)	This is related to echo replies. If your device receives an echo request, it sends an echo reply. If you enter the ping command, your device generates echo requests.
Router Advertisements (10)	These are Router Discovery Protocol messages. If Router Discovery is enabled, your device sends these to announce the IP addresses of the sending interface.
Time to Live Exceeded (11)	If the TTL field in a packet falls to zero, your device sends this message.This occurs when there are too many hops in the path that a packet is traversing.

ICMP messages are enabled on all interfaces by default. You can control the flow of ICMP messages across different interfaces using the **access-list** commands. See **Chapter 37, IPv4 Hardware Access Control List (ACL) Commands** and **Chapter 38, IPv4 Software Access Control List (ACL) Commands**.

Checking IP Connections

To verify connections between networks and network devices, use the ping (Packet Internet Groper) and trace route functions on your device.

Ping

Ping tests the connectivity between two network devices to determine whether each network device can "see" the other device. Echo request packets are sent to the destination addresses and responses are displayed on the console.

If you can ping the end destination, then the physical, Layer 2 and Layer 3 links are functioning, and any difficulties are in the network or higher layers.

If pinging the end destination fails, use traceroute to discover the point of failure in the route to the destination.

To ping a device, use the command:

```
awplus# ping {<hostname>|<ipaddr>}
```

Traceroute

You can use traceroute to discover the route that packets pass between two systems running the IP protocol. Traceroute sends an initial UDP packets with the Time To Live (TTL) field in the IP header set starting at 1. The TTL field is increased by one for every subsequent packet sent until the destination is reached. Each hop along the path between two systems responds with a TTL exceeded packet (ICMP type 11) and from this the path is determined.

To use traceroute, use the command:

```
awplus# traceroute {<ip-addr>|<hostname>}
```

Enter either the hostname or the IP address of the device you are trying to reach.

Chapter 25: IP Addressing and Protocol Commands

Introduction 25.2
Command List 25.3
arp-mac-disparity 25.3
arp-aging-timeout 25.4
arp (IP address MAC) 25.5
arp log 25.6
clear arp-cache 25.9
debug ip packet interface 25.9
ip address 25.11
ip domain-list 25.13
ip domain-lookup 25.14
ip domain-name 25.15
ip gratuitous-arp-link 25.16
ip name-server 25.17
ping 25.18
show arp 25.19
show debugging ip packet 25.20
show hosts 25.21
show ip domain-list 25.21
show ip domain-name 25.22
show ip interface 25.23
show ip name-server 25.24
show ip sockets 25.25
tcpdump 25.27
traceroute 25.28

Introduction

This chapter provides an alphabetical reference of commands used to configure the following protocols:

- Address Resolution Protocol (ARP)
- Domain Name Service (DNS)

For more information see **Chapter 24, Internet Protocol (IP) Addressing and Protocols**.

Command List

arp-mac-disparity

Use this command in Interface Configuration mode for a VLAN interface to enable the reception of ARP packets that contain a multicast MAC address in the sender field.

By default, ARP packets that contain a multicast MAC address in the sender field are dropped. The **no** variant of this command reverts to the default behavior.

Syntax

```
arp-mac-disparity
no arp-mac-disparity
```

Default ARP disparity is disabled. ARP packets with a multicast MAC address in the sender field are dropped.

Mode Interface Configuration for a VLAN interface.

Usage Normally, it is invalid for an ARP request to resolve a multicast MAC address. By default, ARP replies with a multicast MAC addresses are not learned. This command allows control over the learning of dynamic ARPs that resolve to a multicast MAC address.

ARP-MAC disparity may need to be enabled to support multicast network load balancing. The **arp-mac-disparity** command allows ARP replies quoting multicast MAC addresses to be accepted and learned. No **no arp-mac-disparity** command reverts to default behavior.

If the ARP-MAC disparity feature is enabled, then the switch sends traffic to a single port as specified by the ARP entry.

Examples To enable ARP MAC disparity on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity
```

To disable ARP MAC disparity on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity
```

Related Commands

clear arp-cache
show arp

arp-aging-timeout

This command sets a timeout period on dynamic ARP entries associated with a specific interface. If your device stops receiving traffic for the host specified in a dynamic ARP entry, it deletes the ARP entry from the ARP cache after this timeout is reached.

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. Static ARP entries are not aged or automatically deleted.

By default the time limit for dynamic ARP entries is 300 seconds on all interfaces.

The **no** variant of this command sets the time limit to the default of 300 seconds.

Syntax

```
arp-aging-timeout <0-432000>
no arp-aging timeout
```

Parameter	Description
<0-432000>	The timeout period in seconds.

Default 300 seconds (5 minutes)

Mode Interface Configuration for a VLAN interface.

Example To set the ARP entries on interface `vlan30` to time out after two minutes, use the commands:

```
awplus(config)# interface vlan30
awplus(config-if)# arp-aging-timeout 120
```

Related Commands

clear arp-cache
show arp

arp (IP address MAC)

This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the **alias** parameter to allow your device to respond to ARP requests for this IP address.

The **no** variant of this command removes the static ARP entry. Use the **clear arp-cache** command on page 25.9 to remove the dynamic ARP entries in the ARP cache.

Syntax

```
arp <ip-addr> <mac-address> [<port-number>] [alias]
no arp <ip-addr>
```

Parameter	Description
<ip-addr>	IPv4 address of the device you are adding as a static ARP entry.
<mac-address>	MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.
<port-number>	The port number associated with the IP address. Specify this when the IP address is part of a VLAN.
alias	Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4655 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2355.4566 alias
```

Related Commands

clear arp-cache
show arp

arp log

This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of switch ports, VLAN IDs, and IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the default hexadecimal notation (HHHH.HHHH.HHHH), or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of dynamic and static ARP entries in the ARP cache.

Syntax

```
arp log [mac-address-format ieee]
no arp log [mac-address-format ieee]
```

Parameter	Description
`mac-address-format ieee`	Display the MAC address in hexadecimal notation with the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the default hexadecimal format (HHHH.HHHH.HHHH).

Default The ARP logging feature is disabled by default.

Mode Global Configuration

Usage You have the option to change how the MAC address is displayed in the ARP log message, to use the default hexadecimal notation (HHHH.HHHH.HHHH), or the IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) when you apply the **mac-address-format ieee** parameter.

Enter the **arp log** command without the optional **mac-address-format ieee** parameter specified for MAC addresses in the ARP log output to use the default hexadecimal notation (HHHH.HHHH.HHHH).

Enter the **arp log mac-address-format ieee** command for MAC addresses in the ARP log output to use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command (**no arp log**) without the optional **mac-address-format ieee** parameter specified to disable ARP logging on the switch

Use the **no** variant of this command with the optional **mac-address-format ieee** parameter specified (**no arp log mac-address-format ieee**) to disable IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) and revert to the default hexadecimal notation (HHHH.HHHH.HHHH) for MAC addresses in the ARP log output.

To display ARP log messages use the **show log | include ARP_LOG** command.

Examples To enable ARP logging and use the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

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

To disable ARP logging on the switch of MAC addresses displayed using the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and to specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To disable ARP logging on the switch of MAC addresses displayed using the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), and revert to the use of the default hexadecimal notation (HHHH.HHHH.HHHH) instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use following command:

```
awplus# show log | include ARP_LOG
```

Output Below is example output from the **show log | include ARP_LOG** command after enabling ARP logging displaying default hexadecimal notation MAC addresses (HHHH.HHHH.HHHH) using the **arp log** command.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del
0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0030.940e.136b (192.168.2.20)
2010 Apr  6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below is example output from the **show log | include ARP_LOG** command after enabling ARP logging displaying IEEE standard format hexadecimal notation MAC addresses (HH-HH-HH-HH-HH-HH) using the **arp log mac-address format ieee** command.

Figure 25-1: Example output from the show log | include ARP_LOG command

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-
17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-
03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
30-94-0e-13-6b (192.168.2.20)
2010 Apr  6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below are the parameters in output of the **show log | include ARP_LOG** command with an ARP log message format of *<ARP_LOG> <port number> <VLAN ID> <Operation> <MAC> <IP>* after *<date> <time> <severity> <hostname> <program-name>* information.

Table 25-1: Parameters in output of the show log | include ARP_LOG command

Parameter	Description
<ARP_LOG>	Indicates ARP log entry information follows *<date> <time> <severity> <hostname> <program name>* log information.
<port number>	Indicates switch port number for the ARP log entry.
<VLAN ID>	Indicates the VLAN ID for the ARP log entry.
<Operation>	Indicates 'add' if the ARP log entry displays an ARP addition. Indicates 'del' if the ARP log entry displays an ARP deletion.
<MAC>	Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the **arp log** or the **arp log mac-address-format ieee** command.
<IP>	Indicates the IP address for the ARP log entry.

Validation Commands **show running-config**

Related Commands **show log**

clear arp-cache

This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

Syntax `clear arp-cache [<ip-address>]`

Mode Privileged Exec

Usage To display the entries in the ARP cache, use the **show arp** command. To remove static ARP entries, use the no variant of the **arp (IP address MAC)** command on page 25.5.

Example To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

Related Commands
arp-mac-disparity
arp (IP address MAC)
show arp

debug ip packet interface

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

If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no** variant of this command disables the **debug ip interface** command.

Syntax

```
debug ip packet interface {<interface-name>|all}
   [address <ip-address>|verbose|hex|arp|udp|tcp|icmp]

no debug ip packet interface [<interface-name>]
```

Parameter	Description
<interface>	Specify a single Layer 3 interface name (not a range of interfaces) This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface.
`all`	Specify all Layer 3 interfaces on the switch.
<ip-address>	Specify an IPv4 address. If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.

Parameter	Description
`verbose`	Specify **verbose** to output more of the IP packet. If this keyword is specified then more of the packet is shown in the output.
`hex`	Specify **hex** to output the IP packet in hexadecimal. If this keyword is specified, then the output for the packet is shown in hex.
`arp`	Specify **arp** to output ARP protocol packets. If this keyword is specified, then ARP packets are shown in the output.
`udp`	Specify **udp** to output UDP protocol packets. If this keyword is specified then UDP packets are shown in the output.
`tcp`	Specify **tcp** to output TCP protocol packets. If this keyword is specified, then TCP packets are shown in the output.
`icmp`	Specify **icmp** to output ICMP protocol packets. If this keyword is specified, then ICMP packets are shown in the output.

Mode Privileged Exec and Global Configuration

Examples To turn on ARP packet debugging on `vlan1`, 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 `vlan1` and IP address `192.168.2.4`, use the command:

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

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

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

To turn off IP packet interface debugging on interface `vlan2`, use the command:

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

Related Commands **no debug all**
tcpdump
terminal monitor

ip address

This command sets a static IP address on an interface. To set the primary IP address on the interface, specify only **ip address <*ip-address/m*>**. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

Note

Use **show running-config** interface not **show ip interface brief** when you need to view a secondary address configured on an interface. **show ip interface brief** will only show the primary address not a secondary address for an interface.

The **no** variant of this command removes the IP address from the interface. You cannot remove the primary address when a secondary address is present.

Syntax

```
ip address <ip-addr/prefix-length> [secondary] [label <label>]
no ip address <ip-addr/prefix-length> [secondary]
no ip address
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length you are assigning to the interface.
`secondary`	Secondary IP address.
`label`	Adds a user-defined description of the secondary IP address.
<label>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To add the primary IP address `10.10.10.50/24` to the interface `vlan3`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address `10.10.11.50/24` to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address `10.10.11.50/24` to the local loopback interface `lo`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

Related Commands

interface (to configure)
show ip interface
show running-config interface

ip domain-list

This command adds a domain to the DNS list. Domain are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

Syntax

```
ip domain-list <domain-name>
no ip domain-list <domain-name>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage If there are no domains in the DNS list, then your device uses the domain specified with the **ip domain-name** command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

See **“DNS Client” on page 24.6** for information about DNS Client configuration commands.

Example To add the domain `example.net` to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

Related Commands **show ip domain-list**

ip domain-lookup

This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the **ip name-server** command.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

Syntax

```
ip domain-lookup
no ip domain-lookup
```

Mode Global Configuration

Usage The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

See **"DNS Client" on page 24.6** for information about DNS Client configuration commands.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

Related Commands

ip name-server
show hosts
show ip name-server

ip domain-name

This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The **no** variant of this command removes the domain-name previously set by this command.

Syntax

```
ip domain-name <domain-name>
no ip domain-name <domain-name>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage If there are no domains in the DNS list (created using the **ip domain-list** command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

See **“DNS Client” on page 24.6** for information about DNS Client configuration commands.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command. See **Chapter 64, Dynamic Host Configuration Protocol (DHCP) Introduction** for more information about DHCP and DHCP options.

Example To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

Related Commands

show ip domain-list
show ip domain-name

ip gratuitous-arp-link

This command sets the Gratuitous ARP time limit for all switchports. The time limit restricts the sending of Gratuitous ARP packets to one Gratuitous ARP packet within the time in seconds.

Note

This command specifies time between sequences of Gratuitous ARP packets, and time between individual Gratuitous ARP packets occurring in a sequence, to allow legacy support for older devices and interoperation between other devices that are not ready to receive and forward data until several seconds after linkup.

Additionally, jitter has been applied to the delay following linkup, so Gratuitous ARP packets applicable to a given port are spread over a period of 1 second so are not all sent at once. Remaining Gratuitous ARP packets in the sequence occur after a fixed delay from the first one.

Syntax

```
ip gratuitous-arp-link <0-300>
no ip gratuitous-arp-link
```

Parameter	Description
<0-300>	Specify the minimum time between sequences of Gratuitous ARPs and the fixed time between Gratuitous ARPs occurring in a sequence, in seconds. 0 disables the sending of Gratuitous ARP packets. The default is 8 seconds.

Default The default Gratuitous ARP time limit for all switchports is 8 seconds.

Mode Global Configuration

Usage Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport's state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

Examples To disable the sending of Gratuitous ARP packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
```

To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 20
```

Validation Commands **show running-config**

ip name-server

This command adds IPv4 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

Syntax

```
ip name-server <ip-addr>
no ip name-server <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of the DNS server that is being added to the name server list. The address is entered in the form `A.B.C.D`.

Mode Global Configuration

Usage When your device is using its DHCP client for an interface, it can receive Option 6 messages from the DHCP server. This option appends the name server list with more DNS servers.

Examples To allow a device to send DNS queries to a DNS server with the IPv4 address `10.10.10.5`, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 10.10.10.5
```

ping

This command sends a query to another IPv4 host (send Echo Request messages).

Syntax

```
ping [ip] <host> [broadcast] [df-bit {yes|no}] [interval <0-128>]
   [pattern <hex-data-pattern>] [repeat {<1-2147483647>|continuous}]
   [size <36-18024>] [source <ip-addr>] [timeout <1-65535>] [tos <0-
   255>]
```

Parameter	Description
<host>	The destination IP address or hostname.
`broadcast`	Allow pinging of a broadcast address.
`df-bit`	Enable or disable the do-not-fragment bit in the IP header.
`interval` *<0-128>*	Specify the time interval in seconds between sending ping packets. The default is 1.
`pattern` *<hex-data-pattern>*	Specify the hex data pattern.
`repeat`	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
`continuous`	Continuous ping
`size` *<36-18024>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
`source` *<ip-addr>*	The IP address of a configured IP interface to use as the source in the IP header of the ping packet.
`timeout` *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
`tos` *<0-255>*	The value of the type of service in the IP header.

Mode User Exec and Privileged Exec

Example To ping the IP address `10.10.0.5` use the following command:

```
awplus# ping 10.10.0.5
```

show arp

Use this command to display entries in the ARP routing and forwarding table—the ARP cache contains mappings of IP addresses to physical addresses for hosts. To have a dynamic entry in the ARP cache, a host must have used the ARP protocol to access another host.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show arp [security [interface [<interface-list>]]
show arp [statistics [detail][interface [<interface-list>]]
```

Mode User Exec and Privileged Exec

Usage Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output **Figure 25-2: Example output from the show arp command**

```
awplus#show arp

 IP Address       MAC Address    Interface    Port         Type
192.168.10.2     0015.77ad.fad8  vlan1       port1.0.1    dynamic
192.168.20.2     0015.77ad.fa48  vlan2       port1.0.2    dynamic
192.168.1.100    00d0.6b04.2a42  vlan2       port1.0.6    static
```

Table 25-2: Parameters in the output of the show arp command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
MAC Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the **arp (IP address MAC)** command. Dynamic entries are learned from ARP request/reply message exchanges.

Related Commands

arp (IP address MAC)
clear arp-cache

show debugging ip packet

Use this command to show the IP interface debugging status. IP interface debugging is set using the **debug ip packet interface** command.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging ip packet`

Mode User Exec and Privileged Exec

Example To display the IP interface debugging status when the terminal monitor off, use the command:

```
awplus# terminal no monitor
awplus# show debug ip packet
```

Output **Figure 25-3: Example output from the show debugging ip packet command with terminal monitor off**

```
awplus#terminal no monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (stopped)
interface vlan1 arp verbose (stopped)
```

Example To display the IP interface debugging status when the terminal monitor is on, use the command:

```
awplus# terminal monitor
awplus# show debug ip packet
```

Output **Figure 25-4: Example output from the show debugging ip packet command with terminal monitor on**

```
awplus#terminal monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (running)
interface vlan1 arp verbose (running)
```

Related Commands **debug ip packet interface**
terminal monitor

show hosts

This command shows the default domain, domain list, and name servers configured on your device.

Syntax `show hosts`

Mode User Exec and Privileged Exec

Example To display the default domain, use the command:

```
awplus# show hosts
```

Output **Figure 25-5: Example output from the show hosts command**

```
awplus#show hosts
Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

Related Commands
ip domain-list
ip domain-lookup
ip domain-name
ip name-server

show ip domain-list

This command shows the domains configured in the domain list. The DNS client uses the domains in this list to append incomplete hostnames when sending a DNS inquiry to a DNS server.

Syntax `show ip domain-list`

Mode User Exec and Privileged Exec

Example To display the list of domains in the domain list, use the command:

```
awplus# show ip domain-list
```

Output **Figure 25-6: Example output from the show ip domain-list command**

```
awplus#show ip domain-list
alliedtelesis.com
mycompany.com
```

Related Commands
ip domain-list
ip domain-lookup

show ip domain-name

This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

Syntax `show ip domain-name`

Mode User Exec and Privileged Exec

Example To display the default domain configured on your device, use the command:

```
awplus# show ip domain-name
```

Output **Figure 25-7: Example output from the show ip domain-name command**

```
awplus#show ip domain-name
alliedtelesis.com
```

Related Commands **ip domain-name**
ip domain-lookup

show ip interface

Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ip interface [<interface-list>] [brief]
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: ■ an interface, e.g. `vlan2` ■ a continuous range of interfaces separated by a hyphen, e.g. `vlan2-8` or `vlan2-vlan5` ■ a comma-separated list of interfaces or interface ranges, e.g. `vlan2,vlan5,vlan8-10` The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show brief information for the assigned IP address for interface port1.0.2 use the command:

```
awplus# show ip interface port1.0.2 brief
```

To show the IP addresses assigned to vlan2 and vlan3, use the command:

```
awplus# show ip interface vlan2-3 brief
```

Output **Figure 25-8: Example output from the show ip interface brief command**

```
Interface            IP-Address      Status          Protocol
port1.0.2            unassigned      admin up        down
vlan1                192.168.1.1     admin up        running
vlan2                192.168.2.1     admin up        running
vlan3                192.168.3.1     admin up        running
vlan8                unassigned      admin up        down
```

show ip name-server

This command displays a list of IPv4 DNS server addresses that your device will send DNS requests to. This is a static list configured using the **ip name-server** command.

Syntax `show ip name-server`

Mode User Exec and Privileged Exec

Example To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

Output **Figure 25-9: Example output from the show ip name-server command**

```
awplus# show ip name-server
 10.10.0.123
 10.10.0.124
 2001:0db8:010d::1
```

Related Commands **ip domain-lookup**
ip name-server

show ip sockets

Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP, UDP listen sockets, displaying associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip sockets`

Mode Privileged Exec

Usage Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

Example To display ip sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

Output **Figure 25-10: Example output from the show ip sockets command**

```
Socket information

Not showing 40 local connections
Not showing 7 local listening ports

Typ Local Address            Remote Address          State
tcp 0.0.0.0:111              0.0.0.0:*               LISTEN
tcp 0.0.0.0:80               0.0.0.0:*               LISTEN
tcp 0.0.0.0:23               0.0.0.0:*               LISTEN
tcp 0.0.0.0:443              0.0.0.0:*               LISTEN
tcp 0.0.0.0:4743             0.0.0.0:*               LISTEN
tcp 0.0.0.0:873              0.0.0.0:*               LISTEN
tcp :::23                    :::*                    LISTEN
udp 0.0.0.0:111              0.0.0.0:*
udp 226.94.1.1:5405          0.0.0.0:*
udp 0.0.0.0:161              0.0.0.0:*
udp :::161                   :::*
raw 0.0.0.0:112              0.0.0.0:*               112
raw :::58                    :::*                    58
raw :::112                   :::*                    112
```

Table 25-3: Parameters in the output of the show ip sockets command

Parameter	Description
`Not showing <number> local connections`	This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Not showing <number> local listening ports`	This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Typ`	This column displays the type of the socket. Possible values for this column are: `tcp` : IP Protocol 6 `udp` : IP Protocol 17 `raw` : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.
`Local Address`	For TCP and UDP listening sockets this shows the destination IP address and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at: **www.iana.org/assignments/protocol-numbers**
`Remote Address`	For TCP and UDP listening sockets this shows the source IP address (either IPv4 or IPv6) and source TCP or UDP port number for which the socket will accept packets. The address and port are separated by ':'. If the socket will accept packets addressed from any IP address, the IP address will be 0.0.0.0 for IPv4. This is the usual case for a listening socket. Normally for a listen socket any source port will be accepted. This is indicated by ". For active TCP sessions the IP address will display the remote address and port the session was established with. For raw sockets the entry in this column will be 0.0.0.0: for IPv4.

`State`	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are:
	`LISTEN`
	`SYN-SENT`
	`SYN-RECEIVED`
	`ESTABLISHED`
	`FIN-WAIT-1`
	`FIN-WAIT-2`
	`CLOSE-WAIT`
	`CLOSING`
	`LAST-ACK`
	`TIME-WAIT`
	`CLOSED`
	RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

tcpdump

Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press `<ctrl> + c` to stop a running tcpdump.

Syntax `tcpdump <line>`

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see URL **www.tcpdump.org/tcpdump_man.html**

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

Output **Figure 25-11: Example output from the tcpdump command**

```
03:40:33.221337 IP 192.168.1.1 > 224.0.0.13: PIMv2, Hello,
length: 34
1 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Related Commands **debug ip packet interface**

traceroute

Use this command to trace the route to the specified IPv4 host.

Syntax `traceroute {<ip-addr>|<hostname>}`

Parameter	Description
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example

```
awplus# traceroute 10.10.0.5
```

This command applies the functionality of the **no debug ip packet interface** command on page 25.9.

Chapter 26: IPv6 Introduction

Introduction 26.2
Overview 26.2
IPv6 Addresses and Prefixes 26.3
Address Types 26.3
IPv6 Headers 26.4
The Internet Control Message Protocol (ICMPv6) 26.7
IPv6 Routing 26.10
Integration of IPv4 and IPv6 ..... 26.10
IPv6 on your Switch 26.11
Enabling IPv6 ..... 26.11
IPv6 Stateless Address Autoconfiguration (SLAAC) 26.11
IPv6 EUI-64 Addressing 26.11
IPv6 Link-local Addresses 26.12

Introduction

This chapter describes the main features of IPv6, the switch's implementation of IPv6 and how to configure and operate IPv6 on the switch.

This chapter describes the following IPv6 features:

- linking together networks that run IPv6.
- allowing address autoconfiguration of hosts connected to the switch.

Overview

IPv6 is the next generation of the Internet Protocol (IP). It has primarily been developed to solve the problem of the eventual exhaustion of the IPv4 address space, but also offers other enhancements. IPv6 addresses are 16 bytes long, in contrast to IPv4's 4 byte addresses. Other features of IPv6 include:

- Address structure improvements:
  - « globally unique addresses with more levels of addressing hierarchy to reduce the size of routing tables
  - « autoconfiguration of addresses by hosts
  - « improved scalability of multicast routing by adding a "scope" field to multicast addresses
  - « a new type of address, the "anycast address", which sends packets to any one of a group of devices
- Removes the need for packet fragmentation en-route, by dynamic determination of the largest packet size that is supported by every link in the path. A link's MTU (Maximum Transmission Unit) must be at least 1280 bytes, compared with 576 bytes for IPv4.
- Includes a Traffic Class that allow packets to be labeled with an appropriate priority. If the network becomes congested, the lowest priority packets are dropped.
- Includes Flow labels that indicate to intermediate switches and routers that packets are part of a flow, and that a particular flow requires a particular type of service. This feature enables, for example, real-time processing of data streams. It also increases routing speed because the forwarding router or switch needs only to check the flow label, not the rest of the header. The handling indicated by the flow label can be done by the IPv6 Hop-by-Hop header, or by a separate protocol such as RSVP.
- Mandatory authentication and data integrity protocols through IPsec. IPsec is optional in IPv4.

IPv6 Addresses and Prefixes

IPv6 addresses have a hexadecimal format that is made up of eight pairs of octets separated by colons. An example of a valid address is **2001:0db8:0000:0000:0260:0000:97ff:64aa**. In the interests of brevity, addresses can be abbreviated in two ways:

- Leading zeros can be omitted, so this address can be written as **2001:db8:0:0:260:0:97ff:64aa**.
- Consecutive zeros can be replaced with a double colon, so this address can be written as **2001:db8::260:0:97ff:64a**. Note that a double colon can replace any number of consecutive zeros, but an address can contain only one double colon.

Like IPv4 addresses, a proportion of the leftmost bits of the IPv6 address can be used to indicate the subnet, rather than a single node. This part of the address is called the *prefix*. Prefixes provide the equivalent functionality to a subnet mask in IPv4, allowing a subnet to be addressed, rather than a single node. If a prefix is specified, the IPv6 address is followed by a slash and the number of bits that represent the prefix. For example, **2001::/16** indicates that the first 16 bits (**2001**) of the address **2001:0:0:0:0:0:0:0** represent the prefix. **Note that your switch does not allow prefixes greater than 64 bits**.

Like IPv4 addresses, IPv6 addresses are attached to interfaces.

Address Types

IPv6 supports the following address types:

- Unicast
- Multicast
- Anycast

Unicast addresses

A unicast address is attached to a single interface and delivers packets only to that interface. The following special addresses have been defined:

- IPv4-compatible and IPv4-mapped addresses. IPv4-compatible addresses are used to tunnel IPv6 packets across an IPv4 network. IPv4-mapped addresses are used by an IPv6 host to communicate with an IPv4 host. The IPv6 host addresses the packet to the mapped address.
- Link-local addresses can be used on the local network on which the interface is attached. The link-local prefix is **fe80::/10**. Different interfaces on a device may have the same link-local address. The switch will automatically generate a link-local address for all interfaces that are using IPv6. Commands entered to configure link-local addresses that match any automatically generated link-local addresses by the switch will not be executed.

  Enter the **show ipv6 interface** command to display automatically generated link-local addresses not shown in the **running-config**. Automatically generated link-local addresses contain the last six hexadecimal numbers of the MAC address for a given interface.
- The Loopback address, consisting of **::1**, which is the equivalent of the IPv4 loopback address and allows a host to send packets to itself.
- The Unspecified address, consisting of **::**, which is the equivalent of the IPv4 unspecified address and is used as a source address by hosts during the autoconfiguration process.

Anycast addresses

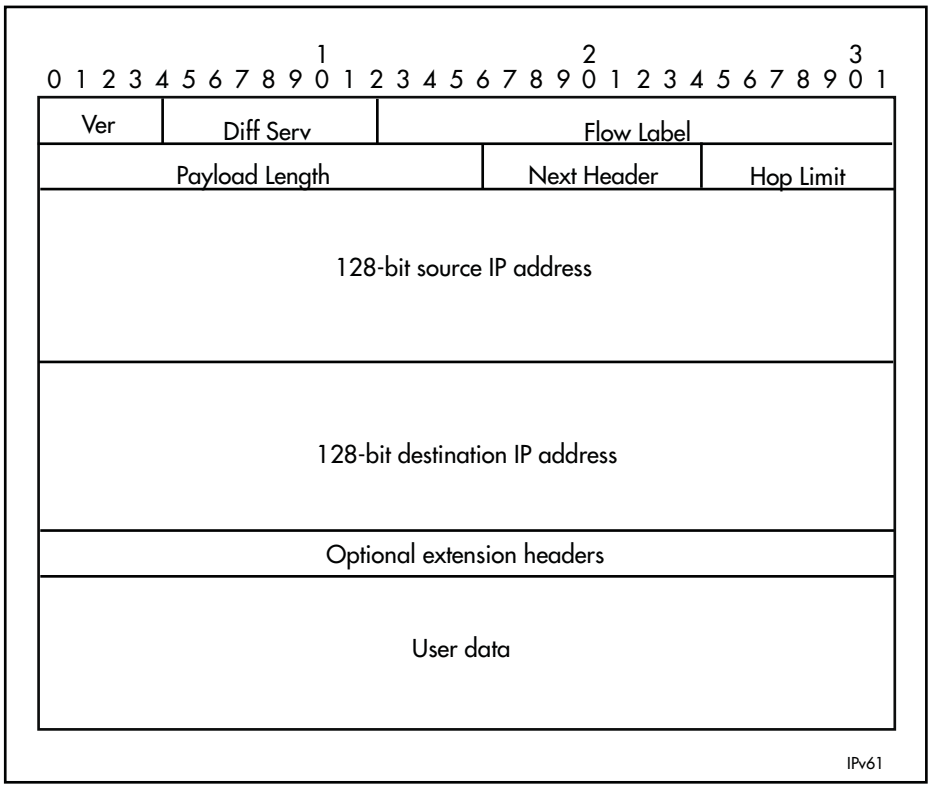
An *anycast* address is a unicast address that is attached to more than one interface. If a packet is sent to an anycast address it is delivered to the nearest interface with that address, with the definition of “nearest” depending on the protocol used for routing.Anycast addresses can be assigned to routers only, and packets cannot originate from an anycast address. A router must be configured to know that it is using an anycast address because the address format cannot be distinguished from that of a unicast address.

Only one anycast address has been predefined: the subnet-router address. The subnet-router address sends messages to the nearest router on a subnet and consists of the subnet’s prefix followed by zeros.

IPv6 Headers

The basic unit of data sent through an internet is called a *packet* in IPv6. A packet consists of a *header* followed by the *data*. The following figure shows the IPv6 packet.

Figure 26-1: IPv6 packet



.

Table 26-1: IPv6 packet - Field Description

Field	Function
Ver	Version of the IP protocol that created the packet. For IPv6, this field has a value of 6.
Differentiated Services	8-bit value that contains the 6-bit DSCP and is used to prioritize traffic as part of a Quality of Service system. For more information, see **"Differentiated Services Architecture" on page 40.4**. Additional information can be found in RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.
Flow Label	20-bit value that indicates the data flow to which this packet belongs.This flow may be handled in a particular way.
Payload Length	Length of the user data portion of the packet. If the data payload is larger than 64 kB, the length is given in the optional "Jumbo Payload" header and the Payload Length header is given a value of zero.
Next Header	Number that indicates the type of header that immediately follows the basic IP header. This header type may be an optional IPv6 extension header, a relevant IPv4 option header, or another protocol, such as TCP or ICMPv6. The IPv6 extension header values are: **0** (Hop-by-Hop Options Header) **43** (IPv6 Routing Header) **44** (IPv6 Fragment Header) **50** (Encapsulating Security Payload) **51** (IPv6 Authentication Header) **59** (No Next Header) **60** (Destination Options Header)
Hop Limit	Field that is the equivalent of the IPv4 Time To Live field, measured in hops.
Source IP address	128-bit IPv6 address of the sender.
Destination IP address	128-bit IPv6 address of the recipient.
Optional extension headers	Headers for less-frequently used information.
User data	Payload.

Basic IPv6 header structure

The headers contain information necessary to move the packet across the Internet. They must be able to cope with missing and duplicated packets as well as possible fragmentation (and reassembly) of the original packet.

IPv6 headers are twice as long as IPv4 headers (40 bytes instead of 20 bytes) and contain four times the address space size (128 bits instead of 32 bits).

They no longer contain the header length, identification, flags, fragment offset, and header checksum fields. Some of these options are placed in extension headers. The Time To Live field is replaced with a hop limit, and the IPv4 Type of Service field is replaced with a Differentiated Services field. The Differentiated Services field contains the DSCP bits, used in a Quality of Service (QoS) regime. The following table explains IPv4 header fields that changed in IPv6.

Changed Field	Description
Type of Service	The type of service that a connection should receive is indicated in IPv6 by the Flow Label field in the IPv6 header.
Fragmentation information (the Identification field, the Flags field and the Fragment Offset field)	In most cases fragmentation does not occur in IPv6. If it does, packets are fragmented at their source and not en route. Therefore, the fragmentation information is contained in an extension header to reduce the size of the basic IPv6 header.
Header Checksum	This option has not been provided in IPv6. This is because transport protocols implement checksums and because of the availability of the IPsec authentication header (AH) in IPv6.
Options	Extension headers handle all the optional values associated with IPv6 packets. The biggest advantage of this scheme is that the size of the basic IP header is a constant.

Extension headers

IPv6 implements many of the less commonly used fields in the IPv4 header (or their equivalents) as extension headers, which are placed after the basic IPv6 header. The length of each header must be a multiple of 8 bytes.

The first extension header is identified by the Next Header field in the basic IPv6 header. Any subsequent extension headers are identified by an 8-bit “Next Header” value at the beginning of the preceding extension header.

IPv6 nodes that originate packets are required to place extension headers in a specific order:

1. The basic IPv6 header. This must come immediately before the extension headers.
2. The Hop-by-Hop header. This specifies options that must be examined by every node in the routing path.
3. A Destination Options header. This is used to specify options to be processed by the first destination or final destination. The destination options header is the only extension header that may be present more than once in the IPv6 packet.
4. The Routing header. This enables a static path to be specified for the packet, if the dynamically-determined path is undesirable.
5. The Fragment header. This indicates that the source node has fragmented the packet, and contains information about the fragmentation.

6. The Authentication header (AH). This verifies the integrity of the packet and its headers.

7. The Encapsulating Security Payload (ESP) header. This encrypts a packet and verifies the integrity of its contents.

8. The Upper Layer Protocol header. This indicates which protocol a higher layer (such as the transport layer) is to process the packet with (for example, TCP).

The Internet Control Message Protocol (ICMPv6)

The Internet Control Message Protocol, ICMPv6, provides a mechanism for error reporting and route discovery and diagnostics. It also conveys information about multicast group membership, a function that is carried out by the Internet Group Management Protocol (IGMP) in IPv4, and performs address resolution, which the Address Resolution Protocol (ARP) performs in IPv4.

Significant aspects of ICMPv6 include neighbor discovery, which enables one device in a network to find out about other nearby devices; and stateless address autoconfiguration, which allows a device to dynamically determine its own IPv6 address.

ICMPv6 is also used to support the Ping v6 (*Packet Internet Groper*) and Trace route v6 functions that are used to verify the connections between networks and network devices. Ping is used to test the connectivity between two network devices to determine whether each network device can "see" the other device. Trace route is used to discover the route used to pass packets between two systems running the IP protocol.

Both of these functions operate almost identically in IPv4 and IPv6. For more information, see **"Ping" on page 24.9**.

Neighbor discovery

Neighbor discovery is an ICMPv6 function that enables a router or a host to identify other devices on its links. This information is then used in address autoconfiguration, to redirect a node to use a more appropriate router if necessary, and to maintain reachability information with its neighbors.

The IPv6 Neighbor Discovery protocol is similar to a combination of the IPv4 protocols ARP, ICMP Router Discovery and ICMP Redirect.

The following table describes packet types involved with neighbor discovery.

Packet Type	Description
router solicitation	Packet in which a host sends out a request for routers to generate advertisements.
router advertisement	Allows routers to advertise their presence and other network parameters. A router sends an advertisement packet in response to a solicitation packet from a host.
neighbor solicitation	Packet in which a node sends a packet to determine the link layer address of a neighbor or to verify that a neighbor is still active.
neighbor advertisement	A response to a neighbor solicitation packet. These packets are also used to notify neighbors of link layer address changes.
redirect	Informs hosts of a better first hop.

To comply with Section 6.2.1 of RFC 2461, *IPv6 Neighbor Discovery*, the router does not generate router advertisements by default.

The following table explains packet types and services.

Packet Type	Description
address resolution	A method for carrying out address autoconfiguration, and is achieved using the Neighbor Solicitation Message and the Neighbor Advertisement Message.
router and prefix discovery	On connection to a link, a node needs to know the address of a router that the node can use to reach the rest of the world. The node also needs to know the prefix (or prefixes) that define the range of IP addresses on its link that it can reach without going through a router. Routers use ICMP to convey this information to hosts, by means of router advertisements. The message may have an option attached (the *source link address* option), which enables the receiving node to respond directly to the router, without performing a neighbor solicitation.
immediate information	The configuration of a router includes a defined frequency at which unsolicited advertisements are sent. If a node wants to obtain information about the nearest router immediately, rather than waiting for the next unsolicited advertisement, the node can send a router solicitation message. Each router that receives the solicitation message sends a router advertisement specifically to the node that sent the solicitation.
redirection	If a node is aware of more than one router that it can use to connect to wider networks, the router to which it sends packets by default does not always represent the most desirable route. ICMPv6 uses the redirect packet to communicate a more effective path to the node.
Neighbor Unreachability Detection (NUD)	A node may issue solicitation requests to determine whether a path is still viable, or may listen in on acknowledgement packets of higher layer protocols, such as TCP. If the node determines that a path is no longer viable, it attempts to establish a new link to the neighbor, or to re-establish the previous link. NUD can be used between any two devices in the network, independent of whether the devices are acting as hosts or routers.

Stateless address autoconfiguration

Stateless address autoconfiguration allows an IPv6-aware device to be plugged into a network without manual configuration with an IP address. This plug and play functionality results in networks that are easier to set up and modify, and simplifies the process of shifting to use a new Internet Service Provider (ISP).

Stateless address autoconfiguration is achieved in a series of steps. Routers and hosts perform the first three steps, which autoconfigure a link-local address. A global address is autoconfigured in the last three steps, which only hosts perform.

On the router or host

1. During system start-up, the node begins autoconfiguration by generating a link-local address for the interface. A link-local address is formed by adding the interface ID to the link-local prefix **fe80::/10** (reference RFC 3513).

   Note

   Different interfaces on a device may have the same link-local address. The switch will automatically generate a link-local address for all interfaces that are using IPv6. Commands entered to configure link-local addresses that match any automatically generated link-local addresses by the switch will not be executed. Enter the show ipv6 interface command to display automatically generated link-local addresses not shown in the running-config. Automatically generated link-local addresses contain the last six hexadecimal numbers of the MAC address for a given interface.

2. The node then transmits a neighbor solicitation message to this address. If the address is already in use, the node that the address belongs to replies with a neighbor advertisement message. The autoconfiguration process stops and manual configuration of the node is then required.

3. If no neighbor advertisement is received, the node concludes that the address is available and assigns it to the chosen interface.

On the host

1. The node then sends one or more router solicitations to detect if any routers are present. Any routers present responds with a router advertisement.

   If no router advertisement is received, the node tries to use DHCP to obtain an address and other configuration information. If no DHCP server responds, the node continues using the link-level address

   If a router advertisement is received, this message informs the node how to proceed with the auto configuration process. The prefix from the router advertisement, if received, is added to the link-level address to form the global unicast IP address.

2. This address is then assigned to the network interface.

   If routers are present, the node continues to receive router advertisements. The node updates its configuration when there are changes in the router advertisements.

IPv6 Routing

Routing in IPv6 is almost identical to IPv4 routing under CIDR, except that the addresses are 128-bit IPv6 addresses instead of 32-bit IPv4 addresses.

Integration of IPv4 and IPv6

IPv6 has been designed in such a way that a smooth transition from IPv4 is possible. The most effective way to ensure this is to use a *dual IP stack*. A node configured as a dual stack system has both a 128-bit IPv6 address and a 32-bit IPv4 address, and so can communicate with nodes running IPv4 and those running IPv6.

Another aspect of the transition is to *tunnel* IPv6 packets through an IPv4 network. IPv6 packets are tunneled simply by encapsulating the IPv6 packet within an IPv4 datagram, and identifying that this datagram is an encapsulated IPv6 packet by giving the datagram a protocol value of 41.

IPv6 on your Switch

This section describes the switch's support for IPv6, and how to configure IPv6 on the switch.

Enabling IPv6

The switch's implementation of IPv6 is disabled by default. To enable IPv6 forwarding, use the **ipv6 forwarding** command on page 27.8.

To display information about IPv6 settings, use the **show ipv6 interface brief** command on page 27.24.

Because the switch implements IPv6 as a dual stack, implementing IPv6 does not affect IPv4 functionality.

IPv6 Stateless Address Autoconfiguration (SLAAC)

The switch's implementation of IPv6 supports SLAAC on an interface. To enable IPv6 SLAAC on an interface, use the **ipv6 address autoconfig** command on page 27.5. SLAAC automatically applies the MAC address of the interface to an IPv6 address for the interface specified.

ipv6 address autoconfig enables automatic configuration of IPv6 addresses on an interface using stateless autoconfiguration, and enables IPv6 processing on an interface.

IPv6 EUI-64 Addressing

The switch's implementation of IPv6 supports EUI-64 addressing. EUI-64 applies an IPv6 address that is based on the MAC address of the interface. The EUI-64 identifiers from the MAC address are used as the least significant 64 bits of a unicast address.

To enable IPv6 EUI-64, use the **ipv6 address** command on page 27.3 specifying the optional **eui64** parameter for an interface.

When configuring SLAAC you must ensure that you set the prefix length to 64 bits on the switch that is advertising the RAs used for address configuration via SLAAC.

Prefix information received in an RA (Router Advertisement) will not be applied to form an IPv6 address via SLAAC unless the prefix length is 64. Since the EUI is 64 bits long, the IPv6 prefix of the advertising device must also be 64 bits. This prefix length setting and behavior is in accordance with RFC 4864, section 5.5.3.

IPv6 Link-local Addresses

The switch's implementation of IPv6 supports IPv6 link-local addresses without global addresses for communications within the local subnetwork. Switches do not forward packets to link-local addresses. To enable IPv6 link-local addresses, use the **ipv6 enable** command on page 27.7. **ipv6 enable** automatically configures an IPv6 link-local address on the interface and enables IPv6 processing on the interface.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the **Link-local addresses** glossary entry, and the **ipv6 enable** command for more information. Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Chapter 27: IPv6 Commands

Command List 27.2
clear ipv6 neighbors 27.2
ipv6 address 27.3
ipv6 address autoconfig 27.5
ipv6 enable 27.7
ipv6 forwarding 27.8
ipv6 nd managed-config-flag 27.9
ipv6 nd minimum-ra-interval 27.10
ipv6 nd other-config-flag 27.11
ipv6 nd prefix 27.12
ipv6 nd ra-interval 27.14
ipv6 nd ra-lifetime 27.15
ipv6 nd reachable-time 27.16
ipv6 nd retransmission-time 27.17
ipv6 nd suppress-ra 27.18
ipv6 neighbor 27.19
ipv6 opportunistic-nd 27.20
ipv6 route 27.21
ping ipv6 ..... 27.22
show ipv6 forwarding 27.23
show ipv6 interface brief 27.24
show ipv6 neighbors 27.25
show ipv6 route 27.26
show ipv6 route summary 27.28
traceroute ipv6 ..... 27.29

Command List

This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see **Chapter 26, IPv6 Introduction**.

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Syntax `clear ipv6 neighbors`

Mode Privileged Exec

Example

```
awplus# clear ipv6 neighbors
```

ipv6 address

Use this command to set the IPv6 address of a VLAN interface and enable IPv6.

Use the optional eui64 parameter to derive the interface identifier of the IPv6 address from the MAC address of the interface. Note that the MAC address of the default VLAN is applied if the interface does not have a MAC address of its own when specifying the eui64 parameter.

Use the no variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax

```
ipv6 address <ipv6-addr/prefix-length> [eui64]
no ipv6 address <ipv6-addr/prefix-length> [eui64]
```

Parameter	Description
<ipv6-addr/prefix-length>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. Note that your switch will not accept prefix lengths greater than 64.
`eui64`	A method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch's MAC address. See the Usage section for more information.

Mode Interface Configuration for a VLAN interface.

Usage If the **eui64** parameter is specified then the lower 64 bits of the IPv6 address are appended with the same address that would be acquired through stateless address autoconfiguration (SLAAC) if the device received an RA (Router Advertisement) specifying this prefix. See **ipv6 address autoconfig** for a detailed command description and examples to enable and disable SLAAC. See also the **IPv6 EUI-64 Addressing** section in **Chapter 26, IPv6 Introduction** for further EUI-64 implementation information.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the **Link-local addresses** glossary entry, and the **ipv6 enable** command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Examples

To assign the IPv6 address `2001:0db8::a2/64` to the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address `2001:0db8::a2/64` from the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the **eui64** derived address in the prefix `2001:db8::/48` to VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# ipv6 address 2001:0db8::/48 eui64
```

To remove the **eui64** derived address in the prefix `2001:db8::/48` from VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# no ipv6 address 2001:0db8::/48 eui64
```

Validation Commands

show running-config
show ipv6 interface brief
show ipv6 route

Related Commands

ipv6 address autoconfig

ipv6 address autoconfig

Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

Syntax

```
ipv6 address autoconfig

no ipv6 address autoconfig
```

Mode Interface Configuration for a VLAN interface.

Usage The **ipv6 address autoconfig** command enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6, but does not enable IPv6 forwarding. See **ipv6 forwarding** command on page 27.8 for further description and examples.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface. When applying SLAAC to an interface, note that the MAC address of the default VLAN is applied to the interface if the interface does not have its own MAC address.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the **Link-local addresses** glossary entry, and the **ipv6 enable** command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address autoconfig
```

Validation Commands
show running-config
show ipv6 interface brief
show ipv6 route

Related Commands
ipv6 address
ipv6 enable

ipv6 enable

Use this command to enable IPv6 on an interface without an IPv6 global address for the interface. This enables IPv6 with a IPv6 link-local address, not an IPv6 global address.

Use the no variant of this command to disable IPv6 on an interface without a global address. Note the no variant of this command does not operate on an interface with an IPv6 global address or an interface configured for IPv6 stateless address autoconfiguration (SLAAC),

Syntax

```
ipv6 enable
no ipv6 enable
```

Mode Interface Configuration for a VLAN interface.

Usage The **ipv6 enable** command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing. Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the **Link-local addresses** glossary entry for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Examples To enable IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 enable
```

Validation Commands
show running-config
show ipv6 interface brief
show ipv6 route

Related Commands
ipv6 address
ipv6 address autoconfig

ipv6 forwarding

Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding. Execute this command globally on your device prior to issuing **ipv6 enable** on individual interfaces.

Use this **no** variant of this command to turn off IPv6 unicast routing for IPv6 packet forwarding. Note IPv6 unicast routing for IPv6 packet forwarding is disabled by default.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Mode Global Configuration

Default IPv6 unicast forwarding is disabled by default.

Usage Enable IPv6 unicast forwarding globally for all interface on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

Examples To enable IPv6 unicast routing, use this command as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the **no** variant of this command as shown below:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

Related Commands **ipv6 enable**

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag, contained within the router advertisement field.

Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.

An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.

Use the **no** variant of this command to reset this command to its default of, *flag unset*.

Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Default Unset

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command on page 27.18. This step is included in the example below.

Example To set the managed address configuration flag on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra
ipv6 nd prefix
ipv6 nd other-config-flag

ipv6 nd minimum-ra-interval

Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for a VLAN interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for a VLAN interface.

Syntax

```
ipv6 nd minimum-ra-interval <seconds>
no ipv6 nd minimum-ra-interval [<seconds>]
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.

Default The RA interval for a VLAN interface is unset by default.

Mode Interface Configuration for a VLAN interface.

Examples To set the minimum RA interval for the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd minimum-ra-interval 60
```

Related Commands

ipv6 nd ra-interval
ipv6 nd suppress-ra
ipv6 nd prefix
ipv6 nd other-config-flag

ipv6 nd other-config-flag

Use this command to set the **other** stateful configuration flag (contained within the router advertisement field) to be used for IPv6 address auto-configuration. This flag is used to request the router to provide information in addition to providing addresses.

Note

Setting the **ipv6 nd managed-config-flag** command on page 27.9 implies that the **ipv6 nd other-config-flag** will also be set.

Use **no** variant of this command to reset the value to the default.

Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Default Unset

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command on page 27.18. This step is included in the example below.

Example To set the IPv6 other-config-flag on the VLAN interface `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra
ipv6 nd prefix
ipv6 nd managed-config-flag

ipv6 nd prefix

Use this command in Interface Configuration mode for a VLAN interface to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration.

Use the **no** parameter with this command to reset the IPv6 prefix for a VLAN interface in Interface Configuration mode.

Syntax

```
ipv6 nd prefix <ipv6-prefix/length>

ipv6 nd prefix <ipv6-prefix/length> [<valid-lifetime>]

ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
   <preferred-lifetime> [no-autoconfig]

ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
   <preferred-lifetime> off-link [no-autoconfig]

no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]
```

Parameter	Description
<ipv6-prefix/length>	The prefix to be advertised by the router advertisement message. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.The default is X:X::/64.
<valid-lifetime>	The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 0 and 4294967295 seconds. The default is 2592000 (30 days). Note that this period should be set to a value greater than that set for the prefix preferred-lifetime.
<preferred-lifetime>	Specifies theIPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered a current (undeprecated) value. After this period, the command is still valid but should not be used in new communications. Set to a value between 0 and 4294967295 seconds. The default is 604800 seconds (7 days). Note that this period should be set to a value less than that set for the prefix valid-lifetime.
`off-link`	Specify the IPv6 prefix off-link flag. The default is *flag set*.
`no-autoconfig`	Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration. The default is *flag set*.
`all`	Specify all IPv6 prefixes associated with the VLAN interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Usage This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Examples The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64`.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64` with a valid lifetime of 10 days and a preferred lifetime of 5 days.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64` with a valid lifetime of 10 days, a preferred lifetime of 5 days and no prefix used for autoconfiguration.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 43200
no-autoconfig
```

The following example resets router advertisements on the VLAN interface `vlan4`, so the address prefix of `2001:0db8::/64` is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

The following example resets all router advertisements on the VLAN interface `vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix all
```

Related Commands **ipv6 nd suppress-ra**

ipv6 nd ra-interval

Use this command to specify the interval between IPv6 Router Advertisements (RA) transmissions.

Use **no** parameter with this command to reset the value to the default value (600 seconds).

Syntax

```
ipv6 nd ra-interval <seconds>

no ipv6 nd ra-interval
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.

Default 600 seconds.

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command on page 27.18 as shown in the example below.

Example To set the advertisements interval on the VLAN interface `vlan4` to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd minimum-ra-interval
ipv6 nd suppress-ra
ipv6 nd prefix

ipv6 nd ra-lifetime

Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

Syntax

```
ipv6 nd ra-lifetime <seconds>
no ipv6 nd ra-lifetime
```

Parameter	Description
<seconds>	Time period in seconds. Valid values are from 0 to 9000. Note that you should set this time period to a value greater than the value you have set using the **ipv6 nd ra-interval** command.

Default 1800 seconds

Mode Interface Configuration for a VLAN interface.

Usage This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Examples To set the advertisement lifetime of 8000 seconds on the VLAN interface `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra
ipv6 nd prefix

ipv6 nd reachable-time

Use this command to specify the reachable time in the router advertisement to be used for detecting reachability of the IPv6 neighbor.

Use the **no** variant of this command to reset the value to default.

Syntax

```
ipv6 nd reachable-time <milliseconds>
no ipv6 nd reachable-time
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000. Setting this value to 0 indicates an unspecified reachable-time.

Default 0 milliseconds

Mode Interface Configuration for a VLAN interface.

Usage This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Example To set the reachable-time in router advertisements on the VLAN interface `vlan4` to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on the VLAN interface `vlan4` to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd reachable-time
```

Related Commands **ipv6 nd suppress-ra**
ipv6 nd prefix

ipv6 nd retransmission-time

Use this command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.

Use the **no** variant of this command to reset the retransmission time to the default (1 second).

Syntax

```
ipv6 nd retransmission-time <milliseconds>
no ipv6 nd retransmission-time [<milliseconds>]
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000.

Default 1000 milliseconds (1 second)

Mode Interface Configuration for a VLAN interface.

Examples To set the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan2` to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan2` to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd retransmission-time
```

Related Commands **ipv6 nd suppress-ra**
ipv6 nd prefix

ipv6 nd suppress-ra

Use this command to inhibit IPv6 Router Advertisement (RA) transmission for the current interface. Router advertisements are used when applying IPv6 stateless auto-configuration.

Use **no** parameter with this command to enable Router Advertisement transmission.

Syntax

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Default Router Advertisement (RA) transmission is suppressed by default.

Mode Interface Configuration for a VLAN interface.

Example To enable the transmission of router advertisements from the VLAN interface `vlan4` on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands **ipv6 nd ra-interval**
ipv6 nd prefix

ipv6 neighbor

Use this command to add a static IPv6 neighbor entry.

Use the **no** variant of this command to remove a specific IPv6 neighbor entry.

Syntax

```
ipv6 neighbor <ipv6-address> <vlan-name> <mac-address> <port-list>
no ipv6 neighbor <ipv6-address> <vlan-name> <port-list>
```

Parameter	Description
<ipv6-address>	Specify the neighbor's IPv6 address in format `X:X::X:X`.
<vlan-name>	Specify the neighbor's VLAN name.
<mac-address>	Specify the MAC hardware address in hexadecimal notation with the format `HHHH.HHHH.HHHH`.
<port-list>	Specify the port number, or port range.

Mode Global Configuration

Usage Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the **clear ipv6 neighbors** command.

Example To create a static neighbor entry for IPv6 address `2001:0db8::a2`, on `vlan 4`, MAC address `0000.cd28.0880`, on `port1.0.6`, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan4
0000.cd28.0880 port1.0.6
```

Related Commands **clear ipv6 neighbors**

ipv6 opportunistic-nd

Use this command to enable opportunistic neighbor discovery for the global IPv6 ND cache. Opportunistic neighbor discovery changes the behavior for unsolicited ICMPv6 ND packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global IPv6 ND cache.

Syntax

```
ipv6 opportunistic-nd
no ipv6 opportunistic-nd
```

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

Related Commands **show ipv6 neighbors**

Validation Commands **show running-config interface**

ipv6 route

Use this command to establish the distance for static routes of a network prefix.

Use the **no** variant of this command to disable the distance for static routes of the network prefix.

Syntax

```
ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|
   <gateway-name>} [<distvalue>]

no ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|
   <gateway-name>} [<distvalue>]
```

Parameter	Description
<dest-prefix/length>	Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the IP gateway (or next hop) address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255.
<gateway-name>	Specifies the name of the gateway (or next hop) interface.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 myintname 32
```

Validation Commands **show running-config**
show ipv6 route

ping ipv6

This command sends a query to another IPv6 host (send Echo Request messages).

Note Use of the `interface` parameter keyword, plus an interface or an interface range, with this command is only valid when pinging an IPv6 link local address.

Syntax

```
ping ipv6 {<host>|<ipv6-address>} [repeat {<1-2147483647>|
    continuous}] [size <10-1452>] [interface <interface-list>]
    [timeout <1-65535>]
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
`repeat`	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
`size` *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
`interface` *<interface-list>*	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet.
`timeout` *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
`repeat`	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
`continuous`	Continuous ping.
`size` *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
`timeout` *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example

```
awplus# ping ipv6 2001:0db8::a2
```

Related Commands traceroute ipv6

show ipv6 forwarding

Use this command to display IPv6 forwarding status.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ipv6 forwarding`

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 forwarding
```

Output **Figure 27-1: Example output from the show ipv6 forwarding command**

```
ipv6 forwarding is on
```

show ipv6 interface brief

Use this command to display brief information about interfaces and the IPv6 address assigned to them.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 interface [brief]
```

Parameter	Description
`brief`	Specify this optional parameter to display brief IPv6 interface information.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 interface brief
```

Output **Figure 27-2: Example output from the show ipv6 interface brief command**

```
awplus#show ipv6 interface brief
Interface     IPv6-Address                                  Status      Protocol
lo            unassigned                                    admin up    running
vlan1         2001:db8::1/48                                admin up    down
              fe80::215:77ff:fee9:5c50/64
```

Related Commands **show interface brief**

show ipv6 neighbors

Use this command to display all IPv6 neighbors.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ipv6 neighbors`

Mode User Exec and Privileged Exec

show ipv6 route

Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 route [connected|database|static|summary|<ipv6-address>|
    <ipv6-addr/prefix-length>)]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/ Prefix-Length. The prefix-length is usually set between 0 and 64.
`<ipv6-prefix/length>`	Displays only the routes for the specified IP prefix.

Mode User Exec and Privileged Exec

Example 1 To display an IP route with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

Output **Figure 27-3: Example output of the show ipv6 route command**

```
IPv6 Routing Table
Codes: C - connected, S - static
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, vlan10
C   2001:db8::a:0:0:0:0/64 via ::, vlan10
C   2001:db8::14:0:0:0:0/64 via ::, vlan20
C   2001:db8::0:0:0:0/64 via ::, vlan30
C   2001:db8::28:0:0:0:0/64 via ::, vlan40
C   2001:db8::fa:0:0:0:0/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan40
C   2001:db8::/64 via ::, vlan20
C   2001:db8::/64 via ::, vlan10
```

Example 2 To display all database entries for an IP route, use the following command:

```
awplus# show ipv6 route database
```

Output **Figure 27-4: Example output of the show ipv6 route database command**

```
IPv6 Routing Table
Codes: C - connected, S - static
       > - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
         [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Use this command to display the summary of the current NSM RIB entries.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 route summary
```

Mode

User Exec and Privileged Exec

Example

To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output

Figure 27-5: Example output from the show ipv6 route summary command

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 4
RouteSource     Networks
connected       4
FIB             5
```

Related Commands

show ip route
show ip route database

traceroute ipv6

Use this command to trace the route to the specified IPv6 host.

Syntax `traceroute ipv6 {<ipv6-addr>|<hostname>}`

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example To run a traceroute for the IPv6 address 2001:0db8::a2, use the following command:

```
awplus# traceroute ipv6 2001:0db8::a2
```

Related Commands ping ipv6

Chapter 28: Route Selection

Introduction 28.2
Types of Routes 28.2
- Interface Routes 28.2
- Static Routes 28.2
- RIP Routes 28.3

RIB and FIB Routing Tables 28.4
- Understanding the Routing Information Base (RIB) 28.4
- Administrative Distance 28.5
- Metric 28.6
- Equal Cost Multipath Routing 28.7
- How AlliedWare Plus Deletes Routes 28.7
- How AlliedWare Plus Adds Routes 28.8
- Troubleshooting Routes not Installed in the RIB 28.9
- Troubleshooting Routes not Installed in the FIB 28.9

Introduction

This chapter describes the route selection process used by the AlliedWare Plus™ Operating System. Understanding the route selection process helps in analyzing and troubleshooting route-related problems.

The process of routing packets consists of selectively forwarding data packets from one network to another. Your device must determine which network to send each packet to, and over which interface to send the packet in order to reach the desired network. This information is contained in your device routes. For each packet, your device chooses the best route it has for that packet and uses that route to forward the packet. In addition, you can define filters to restrict the way packets are sent.

Types of Routes

Your device learns routes from static information entered as part of the configuration process and by listening to any configured routing protocols. The following types of routes are available on your device:

Interface Routes

Your device creates an interface route when you create the interface. This route tells your device to send packets over that interface when the packets are addressed to the interface's subnet.

Static Routes

You can manually enter routes, which are then called static routes. You can use static routes to:

- specify the default route (to 0.0.0.0). If your device does not have a route to the packet's destination, it sends it out the default route. The default route normally points to an external network such as the Internet.
- set up multiple networks or subnets. In this case you define multiple routes for a particular interface, usually a LAN port. This is a method of supporting multiple subnets on a single physical media.

To create a static route, use the command:

```
awplus(config)# ip route <subnet&mask> {<gateway-ip>|
                <interface>} [<distance>]
```

RIP Routes

Your device learns dynamic routes from RIP (Routing Information Protocol). RIP updates these routes as the network topology changes.

In all but the most simple networks, we recommend that you configure RIP. This enables your device to learn routes from other routers and switches on the network, and to respond automatically to changes in network topology.

RIP is a simple distance vector IPv4 routing protocol. It determines the number of hops between the destination and your device, where one hop is one link. Given a choice of routes, RIP uses the route that takes the lowest number of hops. If multiple routes have the same hop count, RIP chooses the first route it finds.

See **Chapter 30, RIP Configuration** for further information about RIP Configuration.

RIB and FIB Routing Tables

Your device maintains its routing information in routing tables that tell your device how to find a remote network or host. Each route is uniquely identified in a table by its IP address, network mask, next hop, interface, protocol, and policy. There are two routing tables populated by your device: the **Routing Information Base** (RIB) and the **Forwarding Information Base** (FIB).

Note Routes in the FIB are used locally but are not advertised to neighbors if they are not also in the RIB.

Routing Information Base

The RIB records **all** the routes that your device has learned. Your device uses the RIB to advertise routes to its neighbor devices and to populate the FIB. It adds routes to this table when:

- you add a static route using the **ip route** command
- one or more routing protocols, such as RIP or OSPF, exchange routing information with other routers or hosts
- your device receives route information from a connected interface
- your device gathers route information from an ICMP redirect message or DHCP message

Understanding the Routing Information Base (RIB)

Use the **show ipv6 route database** command to view the IPv6 RIB.

Use the **show ip route database** command to view the IPv4 RIB.

The RIB in AlliedWare Plus displays all the routes sent to the RIB by the routing protocols, plus all the static and connected routes.

The angle bracket > character in show output indicates which route has been selected as the best route. The best routes are installed in the Forwarding Information Base (FIB).

Routes which have been installed in the software FIB are marked with a star * symbol in show output.

The Administrative Distance and the Metric are seen in the square brackets with **AD** on the left of the backslash and **Metric** to the right of **AD**, so this is shown as: **[AD / Metric]**

See the below list of other information displayed in the RIB:

- Route type
- Prefix and Prefix Length
- Administrative Distance
- Metric
- Next-Hop
- Exit interface
- Uptime

Forwarding Information Base

The RIB populates the **Forwarding Information Base** (FIB) with the best route to each destination. When your device receives an IP packet, and no filters are active that would exclude the packet, it uses the FIB to find the most specific route to the destination. If your device does not find a direct route to the destination, and no default route exists, it discards the packet and sends an ICMP message to that effect back to the source.

A route is only deleted in the FIB if the corresponding prefix is removed from the RIB.

Changes to the software FIB are propagated to the hardware FIB, so the software and hardware FIB tables mirror each other.

The number of FIB table entries also mirror the best selected routes in the RIB.

Viewing table entries

To view the routes in the RIB, use the commands:

```
awplus# show ip route database [connected|rip|static]
```

To view the routes in the FIB, use the command:

```
awplus# show ip route [connected|rip|static|<ip-addr>|<ip-
       addr/prefix-length>]
```

Administrative Distance

When multiple routes are available for the same prefix, the AlliedWare Plus™ Operating System adds the routes with the lowest **administrative distance** to the FIB. The administrative distance is a rank given to a route based on the protocol that the route was received from. The lower the administrative distance, the higher the route preference.

The following table lists the default administrative distances for routing protocols.

Protocols	Distance	Preference
Connected Routes directly connected to an interface.	-	1 (highest)
Static Routes added using the **ip route** command or learned through DHCP options on interfaces using DHCP to obtain an IP address.	1	2
RIP Routes learned from RIP.	120	5
Unknown No traffic will be passed to neighbors via this route.	255	(route is not advertised to neighbors)

For static routes, specify the distance when adding the route, use the command:

```
awplus(config)# ip route <subnet&mask> [<gateway-ip>]
                [<interface>] [<distance>]
```

For RIP routes, enter the Router Configuration mode, and use the command:

```
awplus(config-router)# distance <1-255> [<ip-addr/prefix-
                       length>]
```

This sets the administrative distance for all RIP routes.

You cannot set an administrative distance for connected routes.

Note

AlliedWare Plus™ does not populate routes with an administrative distance of 255 in the FIB (Forwarding Information Base). But AlliedWare Plus™ does populate routes with an administrative distance of 255 in the RIB (Routing Information Base).

See the below examples showing the behavior of a static route with an administrative distance of 255, which is only added to the RIB, as seen from the below show output.

Output **Figure 28-1: Static route with an administrative distance of 255 that is added to the RIB**

```
awplus(config)#ip route 100.0.0.0/24 192.168.1.100 255
awplus(config)#end
awplus#show ip route database

Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

S       100.0.0.0/24 [255/0] via 192.168.1.100, vlan1
C    *> 192.168.1.0/24 is directly connected, vlan1
```

Figure 28-2: Static route with an administrative distance of 255 that is not added to the FIB

```
awplus(config)#ip route 100.0.0.0/24 192.168.1.100 255
awplus(config)#end
awplus#show ip route

Codes: C - connected, S - static, R - RIP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

C       192.168.1.0/24 is directly connected, vlan1
```

Metric

The Metric is used to find the best route from one routing source. In the routing table it is used as the next tie breaker if the Administrative Distance (AD) is equal for the routes in it.

Metrics used by AlliedWare Plus routing protocols

The following metrics are used by AlliedWare IPv4 and IPv6 routing protocols:

IPv4 and IPv6 Routing Protocol	Metric
RIP for IPv4 / RIPng for IPv6	Hop-Count
OSPFv2 for IPv4 / OSPFv3 for IPv6	Cost
BGP for IPv4 / BGP4+ for IPv6	MULTI_EXIT-DISC / IGMP metric to Next-Hop

Equal Cost Multipath Routing

When multiple routes are available for the same prefix within the FIB, then your device uses Equal Cost Multipath Routing (ECMP) to determine how to forward packets.

ECMP allows the AlliedWare Plus™ Operating System to distribute traffic over multiple equal-cost routes to a destination. The software determines that two or more routes are equal cost if they have the same destination IP address and mask. When the software learns such multiple routes, it puts them in an ECMP route group. When it sends traffic to that destination, it distributes the traffic across all routes in the group.

The AlliedWare Plus™ Operating System distributes traffic over the routes one flow at a time, so all packets in a session take the same route. Each equal-cost route group can contain up to eight individual routes. ECMP is only used to select between routes already in the FIB.

By default, each equal-cost route group can contain four routes. You can change this setting by using the command:

```
awplus(config)# maximum-paths <1-8>
```

The maximum path setting determines how many routes with the same prefix value and the same administrative distance that the FIB can contain. Once an equal-cost route group has the maximum number of routes, then the RIB cannot add any further routes to the route group. The device only adds to the group if a route is deleted from the FIB.

To disable ECMP, set the maximum paths value to one.

How AlliedWare Plus Deletes Routes

When the AlliedWare Plus™ Operating System receives a route delete request from a routing protocol, it first deletes the specified route from its RIB. Then it checks if the specified route is in the FIB.

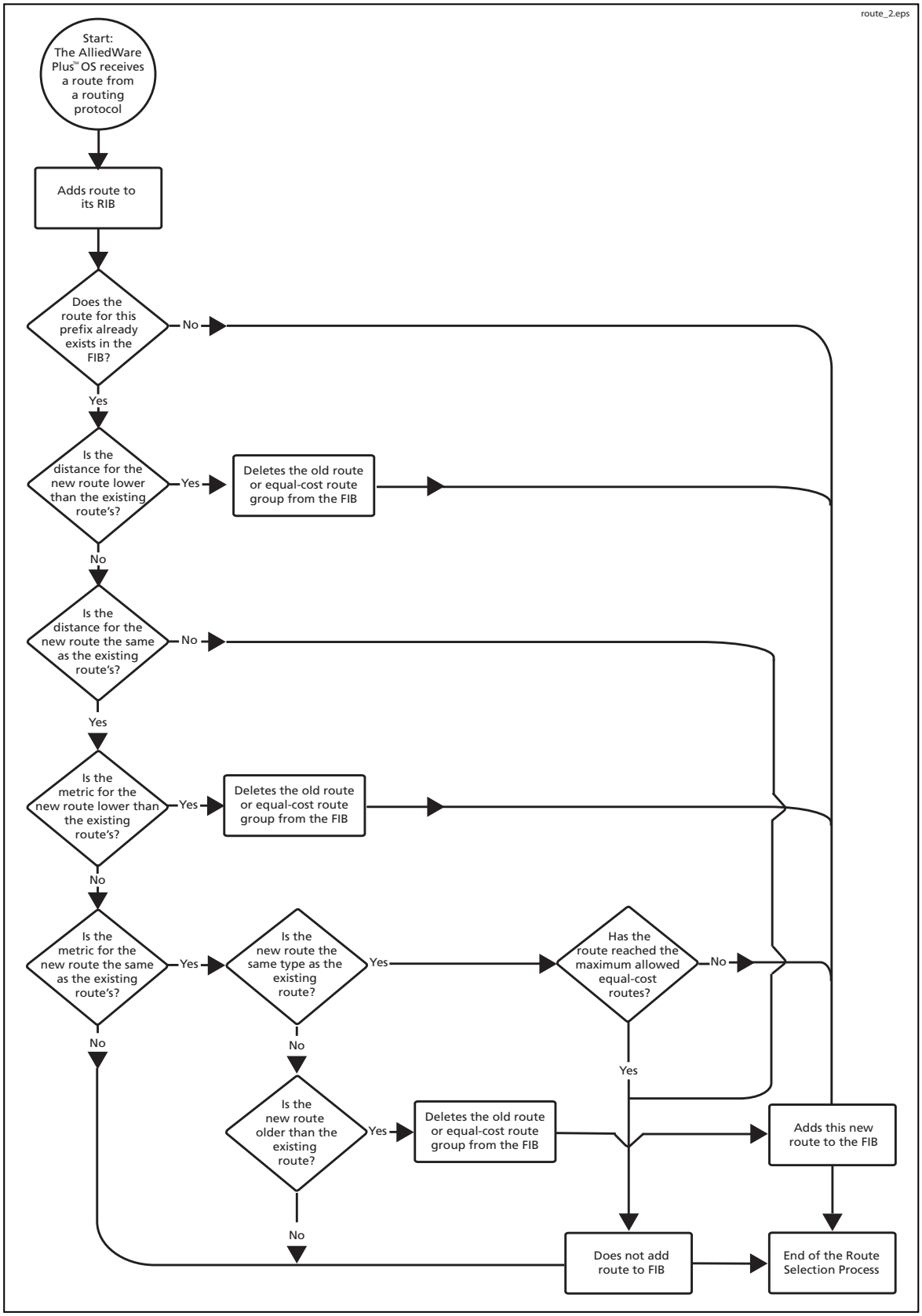
If the route is in the FIB, it deletes it from the FIB and checks if another route is available in its database for the same prefix.

If there is another route in the database, the software installs this route in the FIB. When multiple such routes exist, the software uses the route selection mechanism to choose the best route before adding it to the FIB.

How AlliedWare Plus Adds Routes

The following flow chart shows how the software adds a route to the FIB.

Figure 28-3: How AlliedWare Plus™ adds a route to the FIB



Troubleshooting Routes not Installed in the RIB

Possible reasons why a route is not installed in the RIB are:

- The layer 3 interface is not in the Up state.
- Route oscillation (route flap) is occurring with the route being added and removed frequently.
- The routing process from which the route is learned, has deleted the route.

See the **max-static-routes** command in the **System Configuration and Monitoring Commands** chapter for detailed command description and command example information, where static routes are applied before adding routes to the RIB.

Troubleshooting Routes not Installed in the FIB

Possible reasons why a route is not installed in the FIB are:

- The maximum-paths limit may have been reached (currently supports up to eight equal cost paths being installed).
- The maximum-paths command may be set to a lower value preventing more paths being selected as best.
- The desired route type has a higher AD over another route entry in the RIB, so is not preferred.
- The max-fib-routes command is configured and the maximum number of installed software FIB routes has been reached.

See the **max-fib-routes** command in the **System Configuration and Monitoring Commands** chapter for detailed command description and command example information to control the maximum number of FIB routes configured.

Chapter 29: Routing Commands

Introduction 29.2
Command List 29.3
ip route 29.3
maximum-paths 29.5
show ip route 29.6
show ip route database 29.8
show ip route summary 29.9

Introduction

This chapter provides an alphabetical reference of routing commands that are common across the routing IP protocols.

For more information see **Chapter 28, Route Selection**.

Command List

ip route

This command adds a static route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route from the RIB and FIB.

Syntax

```
ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]
no ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]
```

Parameter	Description
<subnet&mask>	The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats:
	The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation.
	The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length.
<gateway-ip>	The IPv4 address of the gateway device.
<interface>	The interface that connects your device to the network. Enter the name of the VLAN or its VID. The gateway IP address or the interface is required.
<distance>	The administrative distance for the static route in the range <1-255>. Static routes by default have an administrative distance of 1.

Mode Global Configuration

Default The default administrative distance for a static route is 1 for priority over non-static routes.

Usage Administrative distance can be modified so static routes do not take priority over other routes.

Examples To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at “10.10.0.2” with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2 128
```

Related Commands

show ip route
show ip route database

maximum-paths

This command enables ECMP on your device, and sets the maximum number of paths that each route has in the Forwarding Information Base (FIB). ECMP is enabled by default.

The **no** variant of this command sets the maximum paths to the default of 4.

Syntax

```
maximum-paths <1-8>
no maximum-paths
```

Parameter	Description
<1-8>	The maximum number of paths that a route can have in the FIB.

Default By default the maximum number of paths is 4.

Mode Global Configuration

Examples To set the maximum number of paths for each route in the FIB to 5, use the command:

```
awplus# configure terminal
awplus(config)# maximum-paths 5
```

To set the maximum paths for a route to the default of 4, use the command:

```
awplus# configure terminal
awplus(config)# no maximum-paths
```

show ip route

Use this command to display routing entries in the FIB (Forwarding Information Base). The FIB contains the best routes to a destination, and your device uses these routes when forwarding traffic. You can display a subset of the entries in the FIB based on protocol.

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

Syntax

```
show ip route [connected|rip|static|<ip-addr>|<ip-addr/prefix-
    length>]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`static`	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Example To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

Output Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. The first few lines of the output list the possible codes that may be seen with the route entries.

Typically, route entries are composed of the following elements:

- code
- a second label indicating the sub-type of the route
- network or host ip address
- administrative distance and metric
- next hop ip address
- outgoing interface name
- time since route entry was added

Figure 29-1: Example output from the show ip route command

```
Codes: C - connected, S - static, R - RIP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

C       3.3.3.0/24 is directly connected, vlan1
C       10.10.31.0/24 is directly connected, vlan2
C       10.70.0.0/24 is directly connected, vlan4
C       33.33.33.33/32 is directly connected, lo
```

```
C       10.10.31.0/24 is directly connected, vlan2
```

This route entry denotes:

- Route entries for network `10.10.31.0/24` are derived from the IP address of local interface `vlan2`.
- These routes are marked as Connected routes `(C)` and always preferred over routes for the same network learned from other routing protocols.

Related Commands **show ip route database**

show ip route database

This command displays the routing entries in the RIB (Routing Information Base).

When multiple entries are available for the same prefix, RIB uses the routes' administrative distances to choose the best route. All best routes are entered into the FIB (Forwarding Information Base). To view the routes in the FIB, use the **show ip route** command.

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

Syntax

```
show ip route database [connected|rip|static]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`static`	Displays only the static routes you have configured.

Mode User Exec and Privileged Exec

Example To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```

Output **Figure 29-2: Example output from the show ip route database command**

```
Codes: C - connected, S - static, R - RIP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
              > - selected route, * - FIB route, p - stale info

C     *> 10.10.31.0/24 is directly connected, vlan2
S     *> 10.10.34.0/24 [1/0] via 10.10.31.16, vlan2
C     *> 10.30.0.0/24 is directly connected, vlan6
S     *> 11.22.11.0/24 [1/0] via 10.10.31.16, vlan2
S     *> 16.16.16.16/32 [1/0] via 10.10.31.16, vlan2
C     *> 45.45.45.45/32 is directly connected, lo
C     *> 127.0.0.0/8 is directly connected, lo
```

The routes added to the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the * nor the > symbol.

Related Commands **show ip route**

show ip route summary

This command displays a summary of the current RIB (Routing Information Base) entries.

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

Syntax `show ip route summary`

Mode User Exec and Privileged Exec

Example To display a summary of the current RIB entries, use the command:

```
awplus# show ip route summary
```

Output **Figure 29-3: Example output from the show ip route summary command**

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source    Networks
connected       5
Total           8
```

Related Commands **show ip route**
show ip route database

Chapter 30: RIP Configuration

Introduction 30.2
Enabling RIP 30.2
Specifying the RIP Version 30.4
RIPv2 Authentication (Single Key) 30.6
RIPv2 Text Authentication (Multiple Keys) 30.8
RIPv2 md5 authentication (Multiple Keys) 30.12

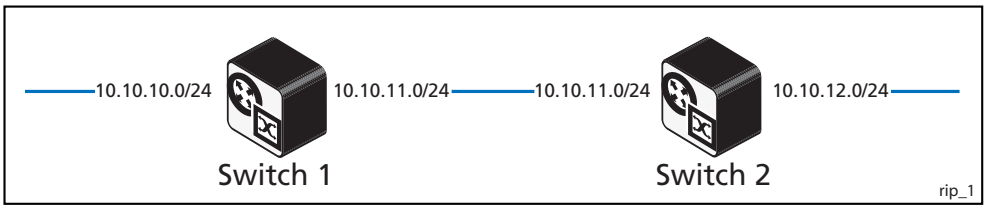
Introduction

This chapter contains basic RIP configuration examples. To see details on the RIP commands used in these examples, or to see the outputs of the validation commands, refer to **Chapter 31, RIP Commands**.

Enabling RIP

This example shows the minimum configuration required for enabling two devices to exchange routing information using RIP. The routing devices in this example are Allied Telesis managed Layer 3 Switches. `Switch 1` and `Switch 2` are two neighbors connecting to network 10.10.11.0/24. Switch 1 and Switch 2 are also connected to networks 10.10.10.0/24 and 10.10.12.0/24 respectively. This example assumes that the devices have already been configured with IP interfaces in those subnets.

To enable RIP, first define the RIP routing process then associate a network with the routing process.



Switch 1

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.10.0/24`	Associate network 10.10.10.0/24 with the RIP process.
`awplus#` `network 10.10.11.0/24`	Associate network 10.10.11.0/24 with the RIP process.

Switch 2

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.11.0/24`	Associate networks with the RIP process
`awplus(config-router)#` `network 10.10.12.0/24`	Associate networks with the RIP process

Names of commands used

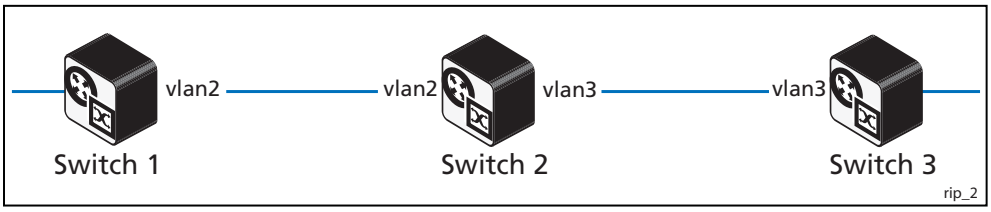
router rip
network (RIP)

Validation commands

show ip rip
show running-config
show ip protocols rip
show ip rip interface
show ip route

Specifying the RIP Version

Configure a router to receive and send specific versions of RIP packets on a VLAN interface. The routing devices in this example are Allied Telesis managed Layer 3 Switches. In this example, Switch 2 is configured to receive and send RIP version 1 and version 2 information on both `vlan2` and `vlan3` interfaces.



Switch 2

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Enable the RIP routing process.
`awplus(config-router)#` `exit`	Return to the Global Configuration mode
`awplus(config)#` `interface vlan2`	Specify vlan2 as an interface you want to configure.
`awplus(config-if)#` `ip rip send version 1 2`	Allow sending RIP version 1 and version 2 packets out of this interface.
`awplus(config-if)#` `ip rip receive version 1 2`	Allow receiving of RIP version 1 and version 2 packets from the vlan2 interface.
`awplus(config-if)#` `exit`	Exit the Interface mode and return to Global Configuration mode to configure the next interface.
`awplus(config)#` `interface vlan3`	Specify interface vlan3 as the interface you want to configure.
`awplus(config-if)#` `ip rip send version 1 2`	Allow sending RIP version 1 and version 2 packets out of this interface.
`awplus(config-if)#` `ip rip receive version 1 2`	Allow receiving of RIP version 1 and version 2 packets from the vlan3 interface.

Names of commands used

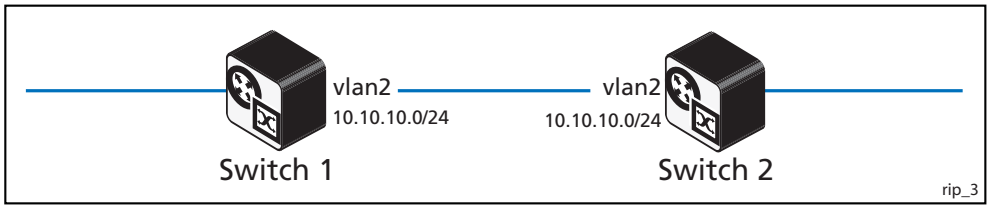
ip rip send version
ip rip receive version

Validation commands

show ip rip
show running-config
show ip protocols rip
show ip rip interface
show ip route

RIPv2 Authentication (Single Key)

AlliedWare Plus™ RIP implementation provides the choice of configuring authentication for a single key or for multiple keys. This example illustrates authentication of the routing information exchange process for RIP using a single key. The routing devices in this example are Allied Telesis managed Layer 3 Switches. Switch 1 and Switch 2 are running RIP and exchange routing updates. To configure single key authentication on Switch 1, specify an interface and then define a key or password for that interface. Next, specify an authentication mode. Any receiving RIP packet on this specified interface should have the same string as password. For an exchange of updates between Switch 1 and Switch 2, define the same password and authentication mode on Switch 2.



Switch 1

`awplus#` `configure terminal`	Enter the Configure mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.10.0/24`	Associate network 10.10.10.0/24 with the RIP process.
`awplus(config-router)#` `redistribute connected`	Enable redistributing from connected routes.
`awplus(config-router)#` `exit`	Exit the Router Configuration mode and return to the Configure mode.
`awplus(config)#` `interface vlan2`	Specify the VLAN interface (vlan2) for authentication.
`awplus(config-if)#` `ip rip authentication string Secret`	Specify the authentication string (Secret) for this interface.
`awplus(config-if)#` `ip rip authentication mode md5`	Specify the authentication mode to be MD5.

Switch 2

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.10.0/24`	Associate network 10.10.10.0/24 with the RIP process.
`awplus(config-router)#` `redistribute connected`	Enable redistributing from connected routes.
`awplus(config-router)#` `exit`	Exit the Router Configuration mode and return to the Global Configuration mode.
`awplus(config)#` `interface vlan2`	Specify the VLAN interface (vlan2) for authentication.
`awplus(config-if)#` `ip rip authentication string Secret`	Specify the authentication string (Secret) on this interface.
`awplus(config-if)#` `ip rip authentication mode md5`	Specify the authentication mode to be MD5.

Names of commands used

ip rip authentication string
ip rip authentication mode
redistribute (RIP)
network (RIP)

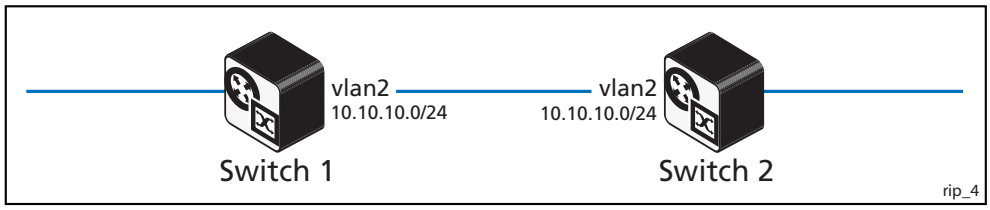
Validation commands

show ip rip
show running-config
show ip protocols rip
show ip rip interface
show ip route

RIPv2 Text Authentication (Multiple Keys)

This example illustrates text authentication of the routing information exchange process for RIP using multiple keys. The routing devices in this example are Allied Telesis managed Layer 3 Switches. Switch 1 and Switch 2 are running RIP and exchanging routing updates. To configure authentication on Switch 1, define a key chain, specify keys in the key chain and then define the authentication string or passwords to be used by the keys. Set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or the set of keys) that will be used for authentication on each interface and also the authentication mode to be used.

Switch 1 accepts all packets that contain any key string that matches one of the key strings included in the specified key chain (within the accept lifetime) on that interface. The key ID is not considered for matching. For additional security, the accept lifetime and send lifetime are configured such that every fifth day the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap. This will accommodate different time-setup on machines. However, the send lifetime does not need to overlap and we recommend not configuring overlapping send lifetimes.



Switch 1

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.10.0/24`	Associate network 10.10.10.0/24 with the RIP process.
`awplus(config-router)#` `redistribute connected`	Enable redistributing of connected routes.
`awplus(config-router)#` `exit`	Exit the Router Configuration mode and return to the Global Configuration mode.
`awplus(config)#` `key chain SUN`	Enter the key chain management mode to add keys to the key chain SUN.
`awplus(config-keychain)#` `key 10`	Add authentication key ID (10) to the key chain SUN.
`awplus(config-keychain-key)#` `key-string Secret`	Specify a password (Secret) to be used by the specified key.

Switch 1(cont.)

`awplus(config-keychain-key)#`	
`accept-lifetime 12:00:00 Mar 2 2007 14:00:00 Mar 7 2007`	Specify the time period during which authentication key string `Secret` can be received. In this case, key string `Secret` can be received from noon of March 2 to 2 pm March 7, 2007.
`awplus(config-keychain-key)#`	
`send-lifetime 12:00:00 Mar 2 2007 12:00:00 Mar 7 2007`	Specify the time period during which authentication key string `Secret` can be send. In this case, key string `Secret` can be received from noon of March 2 to noon of March 7, 2007.
`awplus(config-keychain-key)#`	
`exit`	Exit the keychain-key mode and return to keychain mode.
`awplus(config-keychain)#`	
`key 20`	Add another authentication key (`20`) to the key chain `SUN`.
`awplus(config-keychain-key)#`	
`key-string Earth`	Specify a password (`Earth`) to be used by the specified key.
`awplus(config-keychain-key)#`	
`accept-lifetime 12:00:00 Mar 7 2007 14:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2007.
`awplus(config-keychain-key)#`	
`send-lifetime 12:00:00 Mar 7 2007 12:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be sent. In this case, key string `Secret` can be received from noon of March 7 to noon of March 12, 2007.
`awplus(config-keychain-key)#`	
`end`	Enter Privileged Exec mode.
`awplus#`	
`configure terminal`	Enter the Global Configuration mode.
`awplus(config)#`	
`interface vlan2`	Specify VLAN interface (vlan2) as the interface you want to configure on Switch 1.
`awplus(config-if)#`	
`ip rip authentication key-chain SUN`	Enable RIPv2 authentication on the `vlan2` interface and specify the key chain `SUN` to be used for authentication.
`awplus(config-if)#`	
`ip rip authentication mode text`	Specify text authentication mode to be used for RIP packets. This step is optional, as text is the default mode.

Switch 2

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# router rip	Define a RIP routing process and enter the Router Configuration mode.
awplus(config-router)# network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
awplus(config-router)# redistribute connected	Enable redistributing from connected routes.
awplus(config-router)# exit	Exit the Router Configuration mode and return to the Global Configuration mode.
awplus(config)# key chain MOON	Enter the key chain management mode to add keys to the key chain `MOON`.
awplus(config-keychain)# key 30	Add authentication key ID (`30`) to the key chain `MOON`.
awplus(config-keychain-key)# key-string Secret	Specify a password (`Secret`) to be used by the specified key.
awplus(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2007 14:00:00 Mar 7 2007	Specify the time period during which authentication key string `Secret` can be received. In this case, key string `Secret` can be received from noon of March 2 to 2 pm March 7, 2007.
awplus(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2007 12:00:00 Mar 7 2007	Specify the time period during which authentication key string `Secret` can be send. In this case, key string `Secret` can be received from noon of March 2 to noon of March 7, 2007.
awplus(config-keychain)# key 40	Add another authentication key (`40`) to the key chain `MOON`.
awplus(config-keychain-key)# key-string Earth	Specify a password (`Earth`) to be used by the specified key.
awplus(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2007 14:00:00 Mar 12 2007	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2007.

Switch 2(cont.)

`awplus(config-keychain-key)#`	
`send-lifetime 12:00:00 Mar 7 2007 12:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be sent. In this case, key string `Secret` can be received from noon of March 7 to noon of March 12, 2007.
`awplus(config-keychain-key)#`	
`end`	Enter Privileged Exec mode.
`awplus#`	
`configure terminal`	Enter the Global Configuration mode.
`awplus(config)#`	
`interface vlan2`	Specify the VLAN interface that you want to configure on Switch 2.
`awplus(config-if)#`	
`ip rip authentication key-chain MOON`	Enable RIPv2 authentication on the vlan2 interface, and specify the key chain MOON to be used for authentication.
`awplus(config-if)#`	
`ip rip authentication mode text`	Specify authentication mode to be used for RIP packets. This step is optional, as text is the default mode.

Names of commands used

key chain, **key-string**
accept-lifetime
send-lifetime
ip rip authentication key-chain
ip rip authentication mode

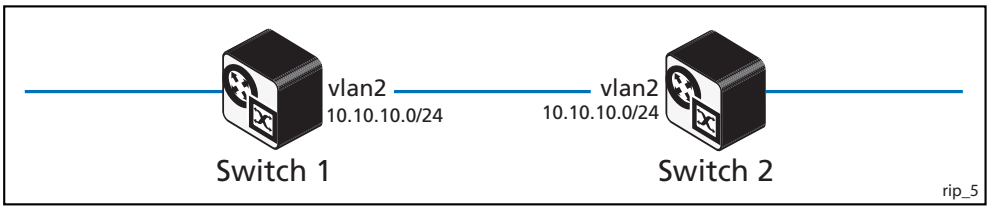
Validation commands

show ip rip
show running-config
show ip protocols rip
show ip rip interface
show ip route

RIPv2 md5 authentication (Multiple Keys)

This example illustrates the md5 authentication of the routing information exchange process for RIP using multiple keys. The routing devices in this example are Allied Telesis managed Layer 3 Switches. Switch 1 and Switch 2 are running RIP and exchange routing updates. To configure authentication on Switch 1, define a key chain, specify keys in the key chain and then define the authentication string or passwords to be used by the keys. Then set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or the set of keys) that will be used for authentication on the interface and the authentication mode to be used. Configure Switch 2 and Switch 3 to have the same key ID and key string as Switch 1 for the time that updates need to be exchanged.

In `md5` authentication, both the key ID and key string are matched for authentication. Switch 1 will receive only packets that match both the key ID and the key string in the specified key chain (within the accept lifetime) on that interface. In the following example, Switch 2 has the same key ID and key string as Switch 1. For additional security, the accept lifetime and send lifetime are configured such that every fifth day the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap; however, the send lifetime should not be overlapping.



Switch 1

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `router rip`	Define a RIP routing process and enter the Router Configuration mode.
`awplus(config-router)#` `network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`awplus(config-router)#` `redistribute connected`	Enable redistributing from connected routes.
`awplus(config-router)#` `exit`	Exit the Router Configuration mode and return to the Global Configuration mode.
`awplus(config)#` `key chain SUN`	Enter the key chain management mode to add keys to the key chain `SUN`.
`awplus(config-keychain)#` `key 1`	Add authentication key ID (`1`) to the key chain `SUN`.

Switch 1(cont.)

`awplus(config-keychain-key)#` `key-string Secret`	Specify a password (`Secret`) to be used by the specified key.
`awplus(config-keychain-key)#` `accept-lifetime 12:00:00 Mar 2 2007 14:00:00 Mar 7 2007`	Specify the time period during which authentication key string `Secret` can be received. In this case, key string `Secret` can be received from noon of March 2 to 2 pm March 7, 2007.
`awplus(config-keychain-key)#` `send-lifetime 12:00:00 Mar 2 2007 12:00:00 Mar 7 2007`	Specify the time period during which authentication key string `Secret` can be send. In this case, key string `Secret` can be received from noon of March 2 to noon of March 7, 2007.
`awplus(config-keychain-key)#` `exit`	Exit the `keychain-key` mode and return to `keychain` mode.
`awplus(config-keychain)#` `key 2`	Add another authentication key (`2`) to the key chain `SUN`.
`awplus(config-keychain-key)#` `key-string Earth`	Specify a password (`Earth`) to be used by the specified key.
`awplus(config-keychain-key)#` `accept-lifetime 12:00:00 Mar 7 2007 14:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2007.
`awplus(config-keychain-key)#` `send-lifetime 12:00:00 Mar 7 2007 12:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be send. In this case, key string `Secret` can be received from noon of March 7 to noon of March 12, 2007.
`awplus(config-keychain-key)#` `end`	Enter Privileged Exec mode.
`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `interface vlan2`	Specify interface `vlan2` as the VLAN interface you want to configure on Switch 1.
`awplus(config-if)#` `ip rip authentication key-chain SUN`	Enable RIPv2 authentication on the `vlan2` interface and specify the key chain `SUN` to be used for authentication.
`awplus(config-if)#` `ip rip authentication mode md5`	Specify the `md5` authentication mode to be used for RIP packets.

Switch 2

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# router rip	Define a RIP routing process and enter the Router Configuration mode.
awplus(config-router)# network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
awplus(config-router)# redistribute connected	Enable redistributing from connected routes.
awplus(config-router)# exit	Exit the Router Configuration mode and return to the Global Configuration mode.
awplus(config)# key chain MOON	Enter the key chain management mode to add keys to the key chain MOON.
awplus(config-keychain)# key 1	Add authentication key ID (1) to the key chain MOON.
awplus(config-keychain-key)# key-string Secret	Specify a password (Secret) to be used by the specified key.
awplus(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2007 14:00:00 Mar 7 2007	Specify the time period during which authentication key string Secret can be received. In this case, key string Secret can be received from noon of March 2 to 2 pm March 7, 2007.
awplus(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2007 12:00:00 Mar 7 2007	Specify the time period during which authentication key string Secret can be send. In this case, key string Secret can be received from noon of March 2 to noon of March 7, 2007.
awplus(config-keychain)# key 2	Add another authentication key (2) to the key chain MOON.
awplus(config-keychain-key)# key-string Earth	Specify a password (Earth) to be used by the specified key.
awplus(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2007 14:00:00 Mar 12 2007	Specify the time period during which authentication key string Earth can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2007.

Switch 2(cont.)

`awplus(config-keychain-key)#`	
`send-lifetime 12:00:00 Mar 7 2007 12:00:00 Mar 12 2007`	Specify the time period during which authentication key string `Earth` can be send. In this case, key string `Secret` can be received from noon of March 7 to noon of March 12, 2007.
`awplus(config-keychain-key)#`	
`end`	Enter Privileged Exec mode.
`awplus#`	
`configure terminal`	Enter the Global Configuration mode.
`awplus(config)#`	
`interface vlan2`	Specify vlan2 as the VLAN interface you want to configure on Switch 2.
`awplus(config-if)#`	
`ip rip authentication key-chain MOON`	Enable RIPv2 authentication on the `vlan2` interface and specify the key chain `MOON` to be used for authentication.
`awplus(config-if)#`	
`ip rip authentication mode md5`	Specify the md5 authentication mode to be used for RIP packets.

Names of commands used

key chain
key-string
accept-lifetime
send-lifetime
ip rip authentication key-chain
ip rip authentication mode

Validation commands

show ip rip
show running-config
show ip protocols rip
show ip rip interface

Chapter 31: RIP Commands

Introduction 31.2
Command List 31.3
accept-lifetime 31.3
alliedware-behavior 31.5
cisco-metric-behavior (RIP) 31.7
clear ip rip route 31.8
debug rip 31.9
default-information originate (RIP) 31.10
default-metric (RIP) 31.11
distance (RIP) 31.12
distribute-list (RIP) 31.13
fullupdate (RIP) 31.14
ip rip authentication key-chain 31.15
ip rip authentication mode 31.18
ip rip authentication string 31.22
ip rip receive-packet 31.24
ip rip receive version 31.25
ip rip send-packet 31.26
ip rip send version 31.27
ip rip send version 1-compatible 31.29
ip rip split-horizon 31.30
key 31.31
key chain 31.32
key-string 31.33
maximum-prefix 31.34
neighbor (RIP) 31.35
network (RIP) 31.36
offset-list (RIP) 31.37
passive-interface (RIP) 31.38
recv-buffer-size (RIP) 31.39
redistribute (RIP) 31.40
restart rip graceful 31.41
rip restart grace-period 31.42
route (RIP) 31.43
router rip 31.44
send-lifetime 31.45
show debugging rip 31.47
show ip protocols rip 31.47
show ip rip 31.48
show ip rip database 31.49
show ip rip interface 31.49
timers (RIP) 31.50
undebug rip 31.51
version 31.52

Introduction

This chapter provides an alphabetical reference of commands used to configure RIP. For more information, see **Chapter 30, RIP Configuration**.

Command List

accept-lifetime

Use this command to specify the time period during which the authentication key on a key chain is received as valid.

Use the **no** variant of this command to remove a specified time period for an authentication key on a key chain as set previously with the **accept-lifetime** command.

Syntax `accept-lifetime <start-date>{<end-date>|duration <seconds>|infinite}`

`no accept-lifetime`

Parameter	Description	
<start-date>	Specifies the start period - time and date in the format DD MMM YYYY or MMM DD YYYY: *<hh:mm:ss> {<day> <month> <year> | <month> <day> <year>}*	
	<hh:mm:ss>	Time of the day when accept-lifetime starts, in hours, minutes and seconds
	<day>	<1-31> Specifies the day of the month to start.
	<month>	Specifies the month of the year to start (the first three letters of the month, for example, Jan).
	<year>	<1993-2035> Specifies the year to start.
<end-date>	Specifies the end period - time and date in the format DD MMM YYYY or MMM DD YYYY: *<hh:mm:ss> {<day> <month> <year> | <month> <day> <year>}*	
	<hh:mm:ss>	Time of the day when lifetime expires, in hours, minutes and seconds.
	<day>	<1-31> Specifies the day of the month to expire.
	<month>	Specifies the month of the year to expire (the first three letters of the month, for example, Feb).
	<year>	<1993-2035> Specifies the year to expire.
<seconds>	<1-2147483646> Duration of the key in seconds.	
infinite	Never expires.	

Mode Keychain-key Configuration

Examples The following examples show the setting of accept-lifetime for `key1` on the key chain named `mychain`.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 Dec 3
2007 04:04:02 Oct 6 2008
```

or:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 3 Dec
2007 04:04:02 6 Oct 2008
```

Related Commands
key
key-string
key chain
send-lifetime

alliedware-behavior

This command configures your device to exhibit AlliedWare behavior when sending RIPv1 response/update messages. Configuring for this behavior may be necessary if you are replacing an AlliedWare device with an AlliedWare Plus device and wish to ensure consistent RIPv1 behavior.

Use the no variant of this command to implement AlliedWare Plus behavior.

This command has no impact on devices running RIPv2. Reception and transmission can be independently altered to conform to AlliedWare standard.

Syntax

```
alliedware-behavior {rip1-send|rip1-recv}
no alliedware-behavior {rip1-send|rip1-recv}
```

Parameter	Description
`rip1-send`	Configures the router to behave in AlliedWare mode when **sending** update messages.
`rip1-recv`	Configures the router to behave in AlliedWare mode when **receiving** update messages.

Default By default when sending out RIPv1 updates on an interface, if the prefix (learned through RIPv2 or otherwise redistributed into RIP) being advertised does not match the subnetting used on the outgoing RIPv1 interface it will be filtered. The **alliedware-behavior** command returns your router's RIPv1 behavior to the AlliedWare format, where the prefix will be advertised as-is.

For example, if a RIPv1 update is being sent over interface 192.168.1.4/26, by default the prefix 192.168.1.64/26 will be advertised, but the prefix 192.168.1.144/28 will be filtered because the mask /28 does not match the interface's mask of /26. If **alliedware-behavior rip1-send** is configured, the prefix 192.168.1.144 would be sent as-is.

Mode Router Configuration

Examples To configure your device for **alliedware-behavior** when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# alliedware-behavior rip1-send
awplus(config-router)# alliedware-behavior rip1-recv
```

To return your device to **AlliedWare Plus**-like behavior when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no alliedware-behavior rip1-send
awplus(config-router)# no alliedware-behavior rip1-recv
```

Validation Commands	**show ip protocols rip** **show running-config**
Related Commands	**fullupdate (RIP)**

cisco-metric-behavior (RIP)

Use this command to enable or disable the RIP routing metric update to conform to Cisco's implementation. This command is provided to allow inter-operation with older Cisco devices that do not conform to the RFC standard for RIP route metrics.

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

Syntax

```
cisco-metric-behavior {enable|disable}
no cisco-metric-behavior
```

Parameter	Description
`enable`	Enables updating the metric consistent with Cisco.
`disable`	Disables updating the metric consistent with Cisco.

Default By default, the Cisco metric-behavior is disabled.

Mode Router Configuration

Examples To enable the routing metric update to behave as per the Cisco implementation, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# cisco-metric-behavior enable
```

To disable the routing metric update to behave as per the default setting, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no cisco-metric-behavior
```

Validation Commands **show running-config**

clear ip rip route

Use this command to clear specific data from the RIP routing table.

Syntax

```
clear ip rip route {<ip-dest-network/prefix-length>|static|connected|
   rip|all}
```

Parameter	Description
<ip-dest-network/prefix-length>	Removes entries which exactly match this destination address from RIP routing table. Enter the IP address and prefix length of the destination network.
`static`	Removes static entries from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`rip`	Removes only RIP routes from the RIP routing table.
`all`	Clears the entire RIP routing table.

Mode Privileged Exec

Usage Using this command with the `all` parameter, clears the RIP table of all the routes.

Examples To clear the route `10.0.0.0/8` from the RIP routing table, use the following command:

```
awplus# clear ip rip route 10.0.0.0/8
```

debug rip

Use this command to specify the options for the displayed debugging information for RIP events and RIP packets.

Use the **no** variant of this command to disable the specified debug option.

Syntax

```
debug rip {events|nsm|<packet>|all}
no debug rip {events|nsm|<packet>|all}
```

Parameter	Description
`events`	RIP events debug information is displayed.
`nsm`	RIP and NSM communication is displayed.
<packet>	`packet [recv|send] [detail]` Specifies RIP packets only.
`recv`	Specifies that information for received packets be displayed.
`send`	Specifies that information for sent packets be displayed.
`detail`	Displays detailed information for the sent or received packet.
`all`	Displays all RIP debug information.

Default Disabled

Mode Privileged Exec and Global Configuration

Example The following example displays information about the RIP packets that are received and sent out from the device.

```
awplus# debug rip packet
```

Related Commands undebug rip

default-information originate (RIP)

Use this command to generate a default route into the Routing Information Protocol (RIP).

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

Syntax

```
default-information originate
no default-information originate
```

Default Disabled

Mode Router Configuration

Usage If routes are being redistributed into RIP and the router's route table contains a default route, within one of the route categories that are being redistributed, the RIP protocol will advertise this default route, irrespective of whether the **default-information originate** command has been configured or not. However, if the router has not redistributed any default route into RIP, but you want RIP to advertise a default route anyway, then use this command.

This will cause RIP to create a default route entry in the RIP database. The entry will be of type RS (Rip Static). Unless actively filtered out, this default route will be advertised out every interface that is sending RIP. Split horizon does not apply to this route, as it is internally generated. This operates quite similarly to the OSPF **default-information originate always** command.

Example

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# default-information originate
```

default-metric (RIP)

Use this command to specify the metrics to be assigned to redistributed RIP routes.

Use the **no** variant of this command to reset the RIP metric back to its default (1).

Syntax

```
default-metric <metric>
no default-metric [<metric>]
```

Parameter	Description
<metric>	<1-16> Specifies the value of the default metric.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Usage This command is used with the **redistribute (RIP)** command to make the routing protocol use the specified metric value for all redistributed routes, regardless of the original protocol that the route has been redistributed from.

Examples This example assigns the cost of 10 to the routes that are redistributed into RIP.

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# default-metric 10
awplus(config-router)# redistribute connected
```

Related Commands **redistribute (RIP)**

distance (RIP)

This command sets the administrative distance for RIP routes. Your device uses this value to select between two or more routes to the same destination obtained from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). See **"Administrative Distance" on page 28.5** for more information.

The **no** variant of this command sets the administrative distance for the RIP route to the default of 120.

Syntax

```
distance <1-255> [<ip-addr/prefix-length>]
no distance [<1-255>] [<ip-addr/prefix-length>]
```

Parameter	Description
<1-255>	The administrative distance value you are setting for this RIP route.
<ip-addr/prefix-length>	The network IP address and prefix-length that you are changing the administrative distance for.

Mode RIP Router Configuration

Examples To set the administrative distance to `8` for the RIP routes within the `10.0.0.0/8` network that match the access-list `mylist`, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distance 8 10.0.0.0/8 mylist
```

To set the administrative distance to the default of `120` for the RIP routes within the `10.0.0.0/8` network that match the access-list `mylist`, use the commands:

```
awplus# configure terminal
awplus (config)# router rip
awplus(config-router)# no distance 8 10.0.0.0/8 mylist
```

distribute-list (RIP)

Use this command to filter incoming or outgoing route updates using the access-list or the prefix-list.

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

Syntax

```
distribute-list {prefix <access-list>} {in|out} [<interface>]
no distribute-list {prefix <access-list>} {in|out}  [<interface>]
```

Parameter	Description
`prefix`	Filter prefixes in routing updates.
`<access-list>`	Specifies the name of the access-list to use.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`<interface>`	The interface on which distribute-list applies. For instance: `vlan2`

Default Disabled

Mode RIP Router Configuration

Usage Filter out incoming or outgoing route updates using an access-list. If you do not specify the name of the interface, the filter will be applied to all interfaces.

Examples In this example the following commands are used to apply an access list called myfilter to filter incoming routing updates in `vlan2`

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distribute-list prefix myfilter in
vlan2
```

Related Commands access-list extended (named)

fullupdate (RIP)

Use this command to specify which routes RIP should advertise when performing a triggered update. By default, when a triggered update is sent, RIP will only advertise those routes that have changed since the last update. When **fullupdate** is configured, the switch advertises the full RIP route table in outgoing triggered updates, including routes that have not changed. This enables faster convergence times, or allow inter-operation with legacy network equipment, but at the expense of larger update messages.

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

Syntax

```
fullupdate
no fullupdate
```

Default By default this feature is disabled.

Mode RIP Router Configuration

Example Use the following commands to enable the fullupdate (RIP) function:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# fullupdate
```

ip rip authentication key-chain

Use this command to enable RIPv2 authentication on an interface and specify the name of the key chain to be used.

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

Syntax

```
ip rip authentication key-chain <key-chain-name>
no ip rip authentication key-chain
```

Parameter	Description
<key-chain-name>	Specify the name of the key chain. This is an alpha-numeric string, but it cannot include spaces.

Mode Interface Configuration for a VLAN interface.

Usage Use this command to perform authentication on the interface. Not configuring the key chain results in no authentication at all.

The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the **ip rip authentication string** command for single key authentication. Use the **ip rip authentication key-chain** command for multiple keys authentication. See **Chapter 30, RIP Configuration** for illustrated RIP configuration examples.

For multiple key authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

Step 1: Define a key chain:

In the Configure mode, identify a key chain with a key chain name using the following command:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

where *<key-chain-name>* is the name of the chain to manage, and should not include spaces.

Step 2: Define the key or keys:

In the Keychain mode, specify a key on this key chain using the following command:

```
awplus(config-keychain)# key <keyid>
```

where *<keyid>* (a decimal number in the range 1 to 2147483647) is the Key Identifier number.

Step 3: Define the authentication string or password:

In the Keychain-key mode, define the password used by a key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

where *<key-password>* is a string of characters that can contain spaces, to be used as a password by the key.

Step 4: Set key management options:

This step can be performed at this stage or later when multiple keys are used. The options are configured in the keychain-key command mode.

Set the time period during which the authentication key on a key chain is received as valid, using the **accept-lifetime** command:

```
awplus(config-keychain-key)# accept-lifetime <START> <END>
```

where *<START>* and *<END>* are the beginning and end of the time period.

Set the time period during which the authentication key on a key chain can be sent, using the **send-lifetime** command:

```
awplus(config-keychain-key)# send-lifetime <START> <END>
```

where *<START>* and *<END>* are the beginning and end of the time period.

Step 5: Enable authentication on an interface:

In the Interface Configuration mode, enable authentication on the VLAN interface `vlan3` and specify the key chain to be used, using the following commands:

```
awplusawpluls# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip authentication key-chain <key-chain-name>
```

where *<key-chain-name>* is a set of valid authentication keys.

Step 6: Specify the mode of authentication for the given interface:

In the Interface Configuration mode for a VLAN interface, specify whether the interface uses text or MD5 authentication using:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example In the following sample multiple keys authentication RIP configuration, a password `toyota` is set for key 1 in key chain `cars`. Authentication is enabled on `vlan2` and the authentication mode is set to MD5:

```
                    awplus# configure terminal
             awplus(config)# key chain cars
        awplus(config-keychain)# key 1
    awplus(config-keychain-key)# key-string toyota
    awplus(config-keychain-key)# accept-lifetime 10:00:00 Apr 08
                                2008 duration 43200
    awplus(config-keychain-key)# send-lifetime 10:00:00 Apr 08
                                2008 duration 43200
    awplus(config-keychain-key)# exit
        awplus(config-keychain)# exit
             awplus(config)# interface vlan2
           awplus(config-if)# ip rip authentication key-chain
                                cars
           awplus(config-if)# ip rip authentication mode md5
            awplus(confi-if)# exit
             awplus(config)# exit
                    awplus#
```

Example In the following example, the VLAN interface `vlan23` is configured to use key-chain authentication with the keychain `mykey`. See the **key** command for a description of how a key chain is created.

```
             awplus# configure terminal
          awplus(config)# interface vlan23
    awplus(config-if)# ip rip authentication key-chain mykey
```

Related Commands

accept-lifetime
send-lifetime
ip rip authentication mode
ip rip authentication string
key
key chain

ip rip authentication mode

Use this command to specify the type of authentication mode used for RIP v2 packets.

Use the **no** variant of this command to restore clear text authentication.

Syntax

```
ip rip authentication mode {md5|text}
no ip rip authentication mode
```

Parameter	Description
`md5`	Uses the keyed MD5 authentication algorithm.
`text`	Specifies clear text or simple password authentication.

Default Text authentication is enabled

Mode Interface Configuration for a VLAN interface.

Usage The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the **ip rip authentication string** command for single key authentication. Use the **ip rip authentication key-chain** command for multiple keys authentication. See **Chapter 30, RIP Configuration** for illustrated RIP configuration examples.

Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

Step 1: Define the authentication string or password

In the Interface Configuration mode for the VLAN interface `vlan2`, specify the authentication string or password used by the key, using the following command:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string <auth-string>
```

where *<auth-string>* is the authentication string or password and it can include spaces.

Step 2: Specify the mode of authentication for the given interface:

In the Interface Configuration mode for VLAN interface `vlan2`, specify if the interface will use text or MD5 authentication, using the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication mode {md5|text}
```

See the sample below to specify `mykey` as the authentication string with MD5

authentication, for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string mykey
awplus(config-if)# ip rip authentication mode md5
```

For multiple keys authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

Step 1: Define a key chain:

In the Global Configuration mode, identify a key chain with a key chain name using the following command:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

where *<key-chain-name>* is the name of the chain to manage, a text string with no spaces.

Step 2: Define the key or keys:

In the Keychain Configuration mode, specify a key on this key chain using the following command:

```
awplus(config-keychain)# key <keyid>
```

where *<keyid>* (a decimal number in the range 1 to 2147483647) is the Key Identifier number.

Step 3: Define the authentication string or password:

In the Keychain-key Configuration mode, define the password used by a key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

where *<key-password>* is a string of characters that can include spaces, to be used as a password by the key.

Step 4: Set key management options:

This step can be performed at this stage or later when multiple keys are used. The options are configured in the Keychain-key Configuration mode.

Set the time period during which the authentication key on a key chain is received as valid, using the **accept-lifetime** command:

```
awplus(config-keychain-key)# accept-lifetime <start> <end>
```

where *<start>* and *<end>* are the beginning and end of the time period.

Set the time period during which the authentication key on a key chain can be sent, using

the **send-lifetime** command:

```
awplus(config-keychain-key)# send-lifetime <start> <end>
```

where <*start*> and <*end*> are the beginning and end of the time period.

Step 5: Enable authentication on an interface:

In the Interface Configuration mode, enable authentication on an interface and specify the key chain to be used, using the following command:

```
awplus(config-if)# ip rip authentication key-chain <key-
                   chain-name>
```

where <*key-chain-name*> is a set of valid authentication keys, as defined in Step 1.

Step 6: Specify the mode of authentication for the given interface:

In the Interface Configuration mode, specify whether the interface uses text or MD5 authentication using:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example 1 In the following sample multiple keys authentication RIP configuration, a password `toyota` is set for key 1 in key chain `cars`. Authentication is enabled on `vlan2` and the authentication mode is set to MD5:

```
                  awplus# configure terminal
            awplus(config)# key chain cars
    awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string toyota
awplus(config-keychain-key)# accept-lifetime 10:00:00 Apr 08
                             2008 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Apr 08 2008
                             duration 43200
awplus(config-keychain-key)# exit
    awplus(config-keychain)# exit
            awplus(config)# interface vlan2
          awplus(config-if)# ip rip authentication key-chain
                             cars
          awplus(config-if)# ip rip authentication mode md5
           awplus(confi-if)# exit
            awplus(config)# exit
                  awplus#
```

Example 2 The following example shows md5 authentication configured on VLAN interface `vlan2`, ensuring authentication of rip packets received on this interface.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication mode md5
```

Related Commands **ip rip authentication string**
ip rip authentication key-chain

ip rip authentication string

Use this command to specify the authentication string or password used by a key.

Use the **no** variant of this command to remove the authentication string.

Syntax

```
ip rip authentication string <auth-string>
no ip rip authentication string
```

Parameter	Description
<auth-string>	The authentication string or password used by a key. It is an alpha-numeric string and can include spaces.

Mode Interface Configuration for a VLAN interface.

Usage The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use this command to specify the password for a single key on an interface. Use the **ip rip authentication key-chain** command for multiple keys authentication. See **Chapter 30, RIP Configuration** for further RIP configuration examples.

Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

Step 1: Define the authentication string or password:

In the Interface Configuration mode, specify the authentication string or password used by the key, using the following commands to configure the authentication string on the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip authentication string <auth-string>
```

where *<auth-string>* is the authentication string or password.

Step 2: Specify the mode of authentication for the given interface:

In the Interface Configuration mode for a VLAN, specify if the interface will use text or MD5 authentication, using the following command:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example See the example below to specify `mykey` as the authentication string with MD5 authentication for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string mykey
awplus(config-if)# ip rip authentication mode md5
```

Example In the following example, the VLAN interface `vlan2` is configured to have an authentication string as `guest`. Any received RIP packet in that interface should have the same string as password.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string guest
```

Related commands **ip rip authentication key-chain**
ip rip authentication mode

ip rip receive-packet

Use this command to configure the interface to enable the reception of RIP packets.

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

Syntax

```
ip rip receive-packet
no ip rip receive-packet
```

Default Receive-packet is enabled

Mode Interface Configuration for a VLAN interface.

Example This example shows packet receiving being turned on for the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip receive-packet
```

Related Commands ip rip send-packet

ip rip receive version

Use this command to specify the version of RIP packets accepted on an interface and override the setting of the version command.

Use the **no** variant of this command to use the setting specified by the **version** command on page 31.52.

Syntax

```
ip rip receive version {[1][2]}
no ip rip receive version
```

Parameter	Description
1	Specifies acceptance of RIP version 1 packets on the interface.
2	Specifies acceptance of RIP version 2 packets on the interface.

Default Version 2

Mode Interface Configuration for a VLAN interface.

Usage This command applies to a specific VLAN interface and overrides any the version specified by the **version** command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Example In the following example, the VLAN interface `vlan3` is configured to receive both RIP version 1 and 2 packets:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip receive version 1 2
```

Related Commands **version**

ip rip send-packet

Use this command to enable sending RIP packets through the current interface.

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

Syntax

```
ip rip send-packet
no ip rip send-packet
```

Default Send packet is enabled

Mode Interface Configuration for a VLAN interface.

Example This example shows packet sending being turned on for the VLAN interface `vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send-packet
```

Related Commands ip rip receive-packet

ip rip send version

Use this command in Interface Configuration mode to specify the version of RIP packets sent on an interface and override the setting of the **version** command. This mechanism causes RIP version 2 interfaces to send multicast packets instead of broadcasting packets.

Use the **no** variant of this command to use the setting specified by the **version** command.

Syntax

```
ip rip send version {1|2|1 2|2 1}
no ip rip send version
```

Parameter	Description
1	Specifies the sending of RIP version 1 packets out of an interface.
2	Specifies the sending of RIP version 2 packets out of an interface.
1 2	Specifies the sending of both RIP version 1 and RIP version 2 packets out of an interface.
2 1	Specifies the sending of both RIP version 2 and RIP version 1 packets out of an interface.

Default RIP version 2 is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to a specific interface and overrides the version specified by the **version** command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces. Selecting version parameters `1 2` or `2 1` sends RIP version 1 and 2 packets.

Use the **ip rip send version 1-compatible** command in an environment where you cannot send multicast packets. For example, in environments where multicast is not enabled and where hosts do not listen to multicast.

Examples In the following example, the VLAN interface `vlan4` is configured to send both RIP version 1 and 2 packets.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 1 2
```

In the following example, the VLAN interface `vlan4` is configured to send both RIP version 2 and 1 packets.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 2 1
```

In the following example, the VLAN interface `vlan4` is configured to send RIP version 1 packets only.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 1
```

In the following example, the VLAN interface `vlan4` is configured to send RIP version 2 packets only.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 2
```

In the following example, the VLAN interface `vlan3` is configured to use the RIP version specified by the **version** command.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip rip send version
```

Related Commands **ip rip send version 1-compatible**
version

ip rip send version 1-compatible

Use this command in Interface Configuration mode to send RIP version 1 compatible packets from a RIP version 2 interfaces to other RIP Interfaces. This mechanism causes RIP version 2 interfaces to send broadcast packets instead of multicasting packets, and is used in environments where multicast is not enabled or where hosts do not listen to multicast.

Use the **no** variant of this command to use the setting specified by the **version** command, and disable the broadcast of RIP version 2 packets that are sent as broadcast packets.

Syntax

```
ip rip send version 1-compatible
no ip rip send version
```

Parameter	Description
`1-compatible`	Specify this parameter to send RIP version 1 compatible packets from a version 2 RIP interface to other RIP interfaces. This mechanism causes version 2 RIP interfaces to broadcast packets instead of multicasting packets.

Default RIP version 2 is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to a specific interface and overrides the version specified by the **version** command.

RIP can be run in version 1 compatible mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Use the **ip rip send version** command in an environment where you can send multicast packets. For example, in environments where multicast is enabled and where hosts listen to multicast.

Examples In the following example, the VLAN interface `vlan2` is configured to send RIP version 1-compatible packets.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip send version 1-compatible
```

In the following example, the VLAN interface `vlan3` is configured to use the RIP version specified by the **version** command.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip rip send version
```

Related Commands **ip rip send version**
version

ip rip split-horizon

Use this command to perform the split-horizon action on the interface. The default is split-horizon poisoned.

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

Syntax

```
ip rip split-horizon [poisoned]
no ip rip split-horizon
```

Parameter	Description
`poisoned`	Performs split-horizon with poisoned reverse.

Default Split horizon poisoned is the default.

Mode Interface Configuration for a VLAN interface.

Usage Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Using the **split horizon** command omits routes learned from one neighbor, in updates sent to that neighbor. Using the **poisoned** parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Example To perform the split-horizon action on, use the following command:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip split-horizon poisoned
```

key

Use this command to manage, add and delete authentication keys in a key-chain.

Use the **no** variant of this command to delete the authentication key.

Syntax

```
key <keyid>
no key <keyid>
```

Parameter	Description
<keyid>	<0-2147483647> Key identifier number.

Mode Keychain Configuration

Usage This command allows you to enter the keychain-key mode where a password can be set for the key.

Example The following example configures a key number 1 and shows the change into a **keychain-key** command mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)#
```

Related Commands

key chain
key-string
accept-lifetime
send-lifetime

key chain

Use this command to enter the key chain management mode and to configure a key chain with a key chain name.

Use the **no** variant of this command to remove the key chain and all configured keys.

Syntax

```
key chain <key-chain-name>
no key chain <key-chain-name>
```

Parameter	Description
<key-chain-name>	Specify the name of the key chain to manage.

Mode Global Configuration

Usage This command allows you to enter the keychain mode from which you can specify keys on this key chain.

Example The following example shows the creation of a key chain named `mychain` and the change into **keychain** mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)#
```

Related Commands

key
key-string
accept-lifetime
send-lifetime

key-string

Use this command to define the password to be used by a key.

Use the **no** variant of this command to remove a password.

Syntax

```
key-string <key-password>
no key-string
```

Parameter	Description
<key-password>	A string of characters to be used as a password by the key.

Mode Keychain-key Configuration

Usage Use this command to specify passwords for different keys.

Examples In the following example, the password for `key1` in the key chain named `mychain` is set to password **prime**:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string prime
```

In the following example, the password for `key1` in the key chain named `mychain` is removed:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# no key-string
```

Related Commands

key
key chain
accept-lifetime
send-lifetime

maximum-prefix

Use this command to configure the maximum number of RIP routes stored in the routing table.

Use the **no** variant of this command to disable all limiting of the number of RIP routes stored in the routing table.

Syntax

```
maximum-prefix <maxprefix> [<threshold>]
no maximum-prefix
```

Parameter	Description
<maxprefix>	<1-65535> The maximum number of RIP routes allowed.
<threshold>	<1-100> Percentage of maximum routes to generate a warning. The default threshold is 75%.

Mode Router Configuration

Example To configure the maximum number of RIP routes to 150, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# maximum-prefix 150
```

neighbor (RIP)

Use this command to specify a neighbor router. It is used for each router to which you wish to send unicast RIP updates.

Use the **no** variant of this command to stop sending unicast updates to the specific router.

Syntax

```
neighbor <ip-address>
no neighbor <ip-address>
```

Parameter	Description
<ip-address>	The IP address of a neighboring router with which the routing information will be exchanged.

Default Disabled

Mode Router Configuration

Usage Use this command to exchange nonbroadcast routing information. It can be used multiple times for additional neighbors.

The **passive-interface (RIP)** command disables sending routing updates on an interface. Use the `neighbor` command in conjunction with the **passive-interface (RIP)** to send routing updates to specific neighbors.

Example To specify the neighbor router to 1.1.1.1, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface vlan1
awplus(config-router)# neighbor 1.1.1.1
```

Related Commands **passive-interface (RIP)**

network (RIP)

Use this command to activate the transmission of RIP routing information on the defined network.

Use the **no** variant of this command to remove the specified network or VLAN as one that runs RIP.

Syntax

```
network {<network-address>[/<subnet-prefix-length>]|<vlan-name>}
no network {<network-address>[/<subnet-mask>]|<vlan-name>}
```

Parameter	Description
<network-address> *[/<subnet-prefix-length>]*	Specifies the network address to run RIP. Entering a subnet mask (or prefix length) for the network address is optional. Where no mask is entered, the switch will attempt to apply a mask that is appropriate to the class (A, B, or C) of the address entered, i.e. an IP address of 10.0.0.0 will have a prefix length of 8 applied to it.
<vlan-name>	Specify a VLAN name with up to 32 alphanumeric characters to run RIP.

Default Disabled

Mode RIP Router Configuration

Usage Use this command to specify networks, or VLANs, to which routing updates will be sent and received. The connected routes corresponding to the specified network, or VLANs, will be automatically advertised in RIP updates. RIP updates will be sent and received within the specified network or VLAN.

Example Use the following commands to activate RIP routing updates on network 172.16.20.0/24:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# network 172.16.20.0/24
```

Related Commands

show ip rip
show running-config
clear ip rip route

offset-list (RIP)

Use this command to add an offset to the **in** and **out** metrics of routes learned through RIP.

Use the **no** variant of this command to remove the offset list.

Syntax

```
offset-list <access-list> {in|out} <offset> [<interface>]
no offset-list <access-list> {in|out} <offset> [<interface>]
```

Parameter	Description
<access-list>	Specifies the access-list number or names to apply.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
<offset>	`<0-16>` Specifies that the offset is used for metrics of networks matching the access list.
<interface>	An alphanumeric string that specifies the interface to match.

Default The default `offset value` is the metric value of the interface over which the updates are being exchanged.

Mode RIP Router Configuration

Usage Use this command to specify the offset value that is added to the routing metric. When the networks match the access list the offset is applied to the metrics. No change occurs if the offset value is zero.

Examples In this example the router examines the RIP updates being sent out from interface `vlan2` and adds `5` hops to the routes matching the ip addresses specified in the access list `8`.

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# offset-list 8 in 5 vlan2
```

Related Commands **access-list (extended numbered)**

passive-interface (RIP)

Use this command to block RIP broadcasts on the VLAN interface.

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

Syntax

```
passive-interface <interface>
no passive-interface <interface>
```

Parameter	Description
<interface>	Specifies the interface name.

Default Disabled

Mode RIP Router Configuration

Usage This command can only be configured for VLAN interfaces.

Examples Use the following commands to block RIP broadcasts on vlan20:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface vlan20
```

Related Commands show ip rip

recv-buffer-size (RIP)

Use this command to run-time configure the RIP UDP (User Datagram Protocol) receive-buffer size to improve UDP reliability by avoiding UDP receive buffer overrun.

Use the **no** variant of this command to reset the configured RIP UDP receive-buffer size to the system default (196608 bits).

Syntax

```
recv-buffer-size <8192-2147483647>

no recv-buffer-size [<8192-2147483647>]
```

Parameter	Description
<8192-2147483647>	Specify the RIP UDP (User Datagram Protocol) buffer size value in bits.

Default 196608 bits is the system default when reset using the **no** variant of this command.

Mode Router Configuration

Examples To run-time configure the RIP UDP, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# recv-buffer-size 23456789

awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no recv-buffer-size 23456789
```

redistribute (RIP)

Use this command to redistribute information from other routing protocols into RIP.

Use the **no** variant of this command to disable the specified redistribution. The parameter **metric** may be used on this command, but has no effect.

Syntax

```
redistribute {connected|static} [metric <0-16>]
no redistribute {connected|static} [metric]
```

Parameter	Description
`connected`	Redistribute from connected routes.
`static`	Redistribute from static routes.
`metric <0-16>`	Optional. Sets the value of the metric that will be applied to routes redistributed into RIP from other protocols. If a value is not specified, and no value is specified using the **default-metric (RIP)** command, the default is one.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Example To apply the metric value 15 to static routes being redistributed into RIP, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# redistribute static metric 15
```

Related Commands **default-metric (RIP)**

restart rip graceful

Use this command to force the RIP process to restart, and optionally set the grace-period.

Syntax `restart rip graceful [grace-period <1-65535>]`

Mode Privileged Exec

Default The default RIP grace-period is 60 seconds.

Usage After this command is executed, the RIP process immediately shuts down. It notifies the system that RIP has performed a graceful shutdown. Routes that have been installed into the route table by RIP are preserved until the specified grace-period expires.

When a **restart rip graceful** command is issued, the RIP configuration is reloaded from the last saved configuration. Ensure you first enter the command **copy running-config startup-config**.

When a master failover happens on a VCStack, the RIP grace-period will apply the larger value of either, the setting's configured value, or its default of 60 seconds.

Example To apply a restart rip graceful setting, grace-period to 100 seconds use the following commands:

```
awplus# copy running-config startup-config
awplus# restart rip graceful grace-period 100
```

rip restart grace-period

Use this command to change the grace period of RIP graceful restart.

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

Syntax

```
rip restart grace-period <1-65535>
no rip restart grace-period <1-65535>
```

Mode Global Configuration

Default The default RIP grace-period is 60 seconds.

Usage Use this command to enable the **Graceful Restart** feature on the RIP process. Entering this command configures a grace period for RIP.

When a master failover happens on a VCStack, the RIP grace-period will be the longest period between the default value (60 seconds is the default RIP grace-period) and the configured RIP grace-period value from this command. So the configured RIP grace-period value will not be used for a VCStack master failover if it is shorter than the default RIP grace-period value.

Example

```
awplus# configure terminal
awplus(config)# rip restart grace-period 200
```

route (RIP)

Use this command to configure static RIP routes.

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

Syntax

```
route <ip-addr/prefix-length>
no route <ip-addr/prefix-length>
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length.

Default No static RIP route is added by default.

Mode RIP Router Configuration

Usage Use this command to add a static RIP route. After adding the RIP route, the route can be checked in the RIP routing table.

Example To create a static RIP route to IP subnet `192.168.1.0/24`, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# route 192.168.1.0/24
```

Related Commands

show ip rip
clear ip rip route

router rip

Use this global command to enter Router Configuration mode to enable the RIP routing process.

Use the **no** variant of this command to disable the RIP routing process.

Syntax

```
router rip
no router rip
```

Mode Global Configuration

Example This command is used to begin the RIP routing process:

```
                awplus# configure terminal
        awplus(config)# router rip
  awplus(config-router)# version 1
  awplus(config-router)# network 10.10.10.0/24
  awplus(config-router)# network 10.10.11.0/24
  awplus(config-router)# neighbor 10.10.10.10
```

Related Commands network (RIP)
version

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Syntax

```
send-lifetime <start-date>{<end-date>|duration <seconds>|infinite}
no send-lifetime
```

Parameter	Description	
<start-date>	Specifies the start period - time and date in the format DD MMM YYYY or MMM DD YYYY: *<hh:mm:ss> {<day> <month> <year> | <month> <day> <year>}*	
	<hh:mm:ss>	Time of the day when send-lifetime starts, in hours, minutes and seconds
	<day>	<1-31> Specifies the day of the month to start.
	<month>	Specifies the month of the year to start (the first three letters of the month, for example, Jan).
	<year>	<1993-2035> Specifies the year to start.
<end-date>	Specifies the end period - time and date in the format DD MMM YYYY or MMM DD YYYY: *<hh:mm:ss> {<day> <month> <year> | <month> <day> <year>}*	
	<hh:mm:ss>	Time of the day when lifetime expires, in hours, minutes and seconds.
	<day>	<1-31> Specifies the day of the month to expire.
	<month>	Specifies the month of the year to expire (the first three letters of the month, for example, Feb).
	<year>	<1993-2035> Specifies the year to expire.
<seconds>	<1-2147483646> Duration of the key in seconds.	
infinite	Never expires.	

Mode Keychain-key Configuration

Example The following example shows the setting of send-lifetime for key1 on the key chain named mychain.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# send-lifetime 03:03:01 Jan 3 2004
04:04:02 Dec 6 2006
```

Related Commands

key
key-string
key chain
accept-lifetime

show debugging rip

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging and RIP nsm debugging.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging rip`

Mode User Exec and Privileged Exec

Usage Use this command to display the debug status of RIP.

Example

```
awplus# show debugging rip
```

show ip protocols rip

Use this command to display RIP process parameters and statistics.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip protocols rip`

Mode User Exec and Privileged Exec

Example

```
awplus# show ip protocols rip
```

Output **Figure 31-1: Example output from the show ip protocols rip command**

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 12
seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface         Send  Recv   Key-chain
   vlan25           2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
Distance: (default is 120
```

show ip rip

Use this command to show RIP routes.

For information on output options, see "Controlling "show" Command Output" on page 1.35.

Syntax

```
show ip rip
```

Mode

User Exec and Privileged Exec

Example

```
awplus# show ip rip
```

Output

Figure 31-2: Example output from the show up rip command

```
awplus#show ip rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static
       C - Connected, S - Static, O - OSPF, B - BGP
Network        Next Hop Metric From If   Time
C 10.0.1.0/24             1      vlan20
S 10.10.10.0/24           1      vlan20
C 10.10.11.0/24           1      vlan20
S 192.168.101.0/24        1      vlan20
R 192.192.192.0/24        1      --
```

Related Commands

route (RIP)
network (RIP)
clear ip rip route

show ip rip database

Use this command to display information about the RIP database.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip rip database [full]`

Parameter	Description
`full`	Specify the full RIP database including sub-optimal RIP routes.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rip database
awplus# show ip rip database full
```

Related Commands **show ip rip**

show ip rip interface

Use this command to display information about the RIP interfaces. You can specify an interface name to display information about a specific interface.

Syntax `show ip rip interface [<interface>]`

Parameter	Description
<interface>	The interface to display information about. For instance: `vlan2`.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rip interface
```

timers (RIP)

Use this command to adjust routing network timers.

Use the **no** variant of this command to restore the defaults.

Syntax

```
timers basic <update> <timeout> <garbage>
no timers basic
```

Parameter	Description
<update>	<5-2147483647> Specifies the period at which RIP route update packets are transmitted. The default is 30 seconds.
<timeout>	<5-2147483647> Specifies the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
<garbage>	<5-2147483647> Specifies the routing garbage collection timer in seconds. The default is 120 seconds.

Default Enabled

Mode RIP Router Configuration

Usage This command adjusts the RIP timing parameters.

The update timer is the time between sending out updates, that contain the complete routing table, to every neighboring router.

If an update for a given route has not been seen for the time specified by the timeout parameter, that route is no longer valid. However, it is retained in the routing table for a short time, with metric 16, so that neighbors are notified that the route has been dropped.

When the time specified by the garbage parameter expires the metric 16 route is finally removed from the routing table. Until the garbage time expires, the route is included in all updates sent by the router.

All the routers in the network must have the same timers to ensure the smooth operation of RIP throughout the network.

Examples To adjust router network timers to 30 180 120, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# timers basic 30 180 120
```

undebug rip

Use this command to disable the options set for debugging information of RIP events, packets and communication between RIP and NSM.

This command has the same effect as the **no debug rip** command.

Syntax `undebug rip {all|events|nsm|<packet>}`

Parameter	Description
`all`	Disables all RIP debugging.
`events`	Disables the logging of RIP events.
`nsm`	Disables the logging of RIP and NSM communication.
<packet>	`packet [recv|send] [detail]` Disables the debugging of RIP packets.
`recv`	Disables the logging of received packet information.
`send`	Disables the logging of sent packet information.
`detail`	Disables the logging of sent or received RIP packets.

Mode Privileged Exec

Example To disable the options set for debugging RIP information events, use the following command:

```
awplus# undebug rip packet
```

Related Commands **debug rip**

version

Use this command to specify a RIP version used globally by the router.

Use the **no** variant of this command to restore the default version.

Syntax

```
version {1|2}
no version
```

Parameter	Description
1|2	Specifies the version of RIP processing.

Default Version 2

Mode RIP Router Configuration

Usage RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Setting the version command has no impact on receiving updates, only on sending them. The **ip rip send version** command overrides the value set by the **version** command on an interface-specific basis. The **ip rip receive version** command allows you to configure a specific interface to accept only packets of the specified RIP version. The **ip rip receive version** command and the **ip rip send version** command override the value set by this command.

Examples To specify a RIP version, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# version 1
```

Validation Commands **show running-config**

```
awplus#show running-config
!
router rip
 version 1
!
```

Related Commands **ip rip receive version**
ip rip send version

Part 4: Multicast Applications

- Chapter 32 IGMP Snooping Introduction
- Chapter 33 IGMP Snooping Commands
- Chapter 34 MLD Snooping Introduction and Configuration
- Chapter 35 MLD Snooping Commands

Chapter 32: IGMP Snooping Introduction

Introduction 32.2
IGMP 32.3
Joining a Multicast Group (Membership Report) 32.4
Staying in the Multicast Group (Query Message) 32.4
Leaving the Multicast Group (Leave Message) 32.4
IGMP Snooping 32.5
How IGMP Snooping Operates 32.5
IGMP Snooping and Querier Configuration Example 32.6
Query Solicitation 32.9
How Query Solicitation Works 32.9
Query Solicitation Operation 32.9
Speeding up IGMP Convergence in a Non-Looped Topology 32.12
Enabling Query Solicitation on Multiple Switches in a Looped Topology 32.12

Introduction

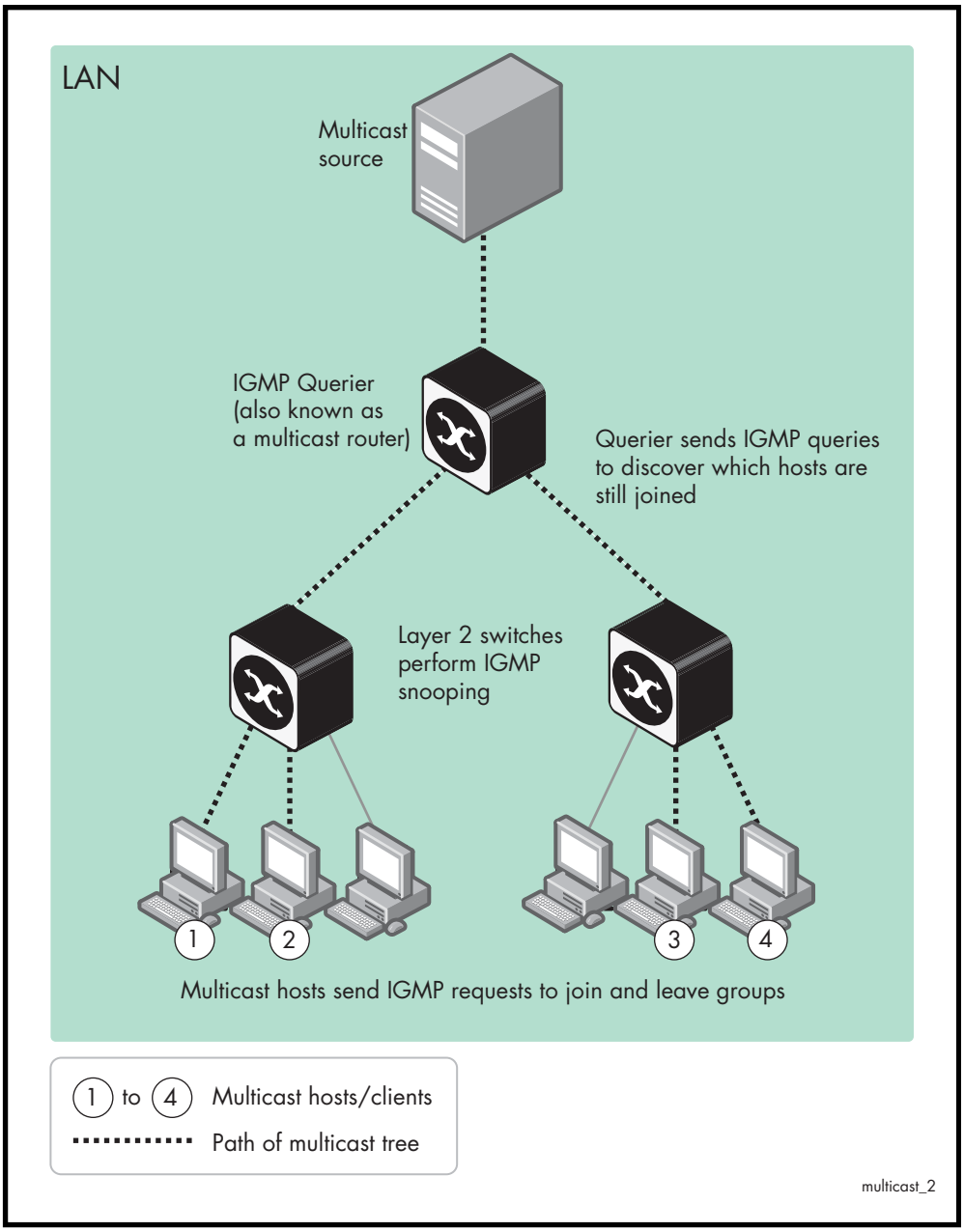
This chapter provides information about Internet Group Management Protocol (IGMP) Snooping, and an introduction to the Query Solicitation feature when used with IGMP Snooping. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to **Chapter 33, IGMP Snooping Commands**.

Your switch does not support IGMP but does support IGMP Snooping.

IGMP

Internet Group Management Protocol (IGMP) is the protocol that hosts use to indicate that they are interested in receiving a particular multicast stream. An example of a multicast system within a single Layer 2 LAN is shown in **Figure 32-1**.

Figure 32-1: Multicast system within a single LAN



Joining a Multicast Group (Membership Report)

When a host wants to receive a stream, referred to as “joining a group”, it sends out an IGMP packet containing the address of the group it wants to join. This packet is called an IGMP Membership report, often referred to as a “join packet”. This packet is forwarded through the LAN to the local IGMP querier, which is typically a router. Once the querier has received an IGMP join message, it knows to forward the multicast stream to the host. If it is not already receiving the stream, it must tell the devices between itself and the multicast source, which may be some hops away from the querier, that it wishes to receive the stream. This might involve a process of using Layer 3 multicast protocols to signal across a WAN, or it might be as simple as receiving a stream from a locally connected multicast server.

Your switch does not support IGMP but does support IGMP Snooping.

Staying in the Multicast Group (Query Message)

The Query message is used by a querier to determine whether hosts are still interested in an IGMP group. At certain time intervals (the default is 125 seconds), the querier sends an IGMP query message onto the local LAN. The destination address of the query message is a special “all multicast groups” address. The purpose of this query is to ask “Are there any hosts on the LAN that wish to remain members of multicast groups?” After receiving an IGMP query, any host that wants to remain in a multicast group must send a new join packet for that group. If a host is a member of more than one group, then it sends a join message for each group it wants to remain a member of. The querier looks at the responses it receives to its query, and compares these to the list of multicast streams that it is currently registered to forward. If there are any items in that list for which it has not received query responses, it will stop forwarding those streams. Additionally, if it is receiving those streams through a Layer 3 network, it will send a Layer 3 routing protocol message upstream, asking to no longer receive that stream.

Leaving the Multicast Group (Leave Message)

How a host leaves a group depends on the IGMP version that it is using. Under IGMP version 1, when a host has finished with a data stream, the local querier continues to send the stream to the host until it sends out the next query message and receives no reply back from the host. IGMP version 2 introduced the Leave message. This allows a host to explicitly inform its querier that it wants to leave a particular multicast group. When the querier receives the Leave message, it sends out a group specific query asking whether any hosts still want to remain members of that specific group. If no hosts respond with join messages for that group, then the querier knows that there are no hosts on its LAN that are still members of that group. This means that for that specific group, it can ask to be pruned from the multicast tree. IGMP version 3 removed the Leave message. Instead a host leaves a group by sending a join message with no source specified.

IGMP Snooping

IGMP Snooping is a way for Layer 2 switches to reduce the amount of multicast traffic on a LAN. The AlliedWare Plus implementation of IGMP Snooping is compatible with networks running all IGMP versions.

Without IGMP Snooping, Layer 2 switches handle IP multicast traffic in the same manner as broadcast traffic and forward multicast frames received on one port to all other ports in the same VLAN. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic, by looking into IGMP packets to learn which attached hosts need to receive which multicast groups. This allows the switch to forward multicast traffic only out the appropriate ports. If it sees multiple reports sent for one group, it will forward only one of them.

How IGMP Snooping Operates

IGMP Snooping operates similarly to the multicast protocols. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the list of ports that are listening to the multicast group. When the switch hears an IGMP leave, it removes the host's port from the list, after the completion of the leave process as described in **"Leaving the Multicast Group (Leave Message)" on page 32.4**. When there are no hosts listening to a group, the switch informs the local querier to stop sending that group's multicast stream.

IGMP Snooping allows query messages to be forwarded to all ports. The hosts that still require the stream respond to the queries by sending reports. The switch intercepts these. Depending on configuration settings, the switch may just forward the reports directly on to the querier, or it may proxy report on behalf of the group, only forwarding on one consolidated report for each group.

By default, IGMP Snooping is enabled both globally and on all VLANs.

Note

IGMP Snooping cannot be disabled on an interface if IGMP Snooping has already been disabled globally. IGMP Snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.

To disable IGMP Snooping either		
1.	`awplus#` `configure terminal`	Enter Global Configuration mode.
2.	`awplus(config)#` `no ip igmp snooping`	Disable IGMP Snooping globally.
or		
1.	`awplus#` `configure terminal`	Enter Global Configuration mode.
2.	`awplus(config)#` `interface <vlan-name>`	Enter Interface Configuration mode for a specific VLAN.
3.	`awplus(config-if)#` `no ip igmp snooping`	Disable IGMP Snooping for a specific VLAN.

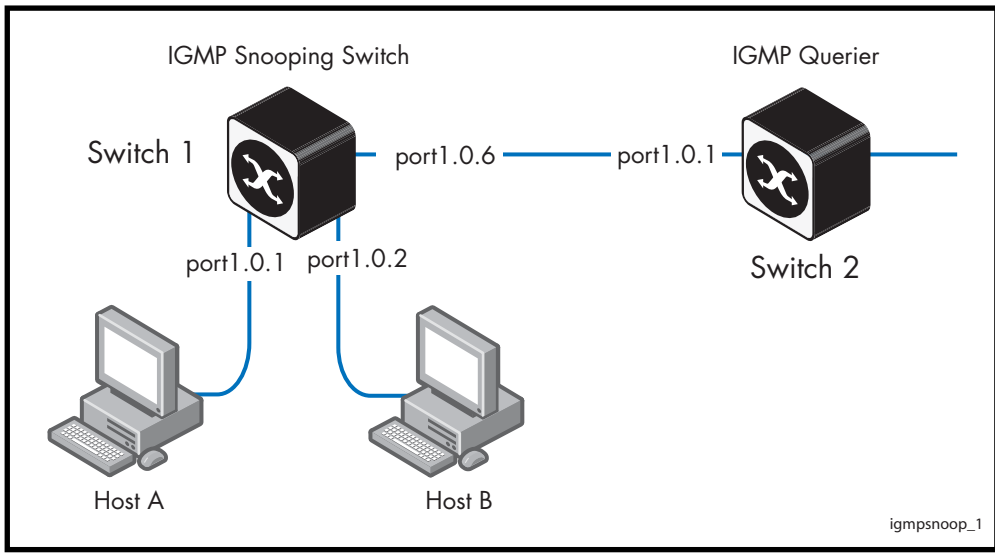
IGMP Snooping and Querier Configuration Example

This example describes the configuration of IGMP Snooping on a switch (Switch 1). Host A and Host B are both members of the same multicast group. In this network, Switch 2 is an IGMP Querier and is an x-series switch, such as an x510. Its configuration is not given here.

To enable IGMP Snooping on an interface:

- Enable IGMP Snooping globally, if necessary. IGMP Snooping is enabled by default.
- Enable IGMP Snooping on the desired interfaces, if necessary. IGMP Snooping is enabled on all interfaces by default.
- Statically configure ports that are connected to routers if necessary.

Figure 32-2: IGMP Snooping configuration example



As a result of this configuration:

- Membership reports are generated by hosts. The IGMP Snooping switch will forward the membership reports to its router port. Queries received by the IGMP Snooping switch from the IGMP Querier on port1.0.6 are forwarded by the IGMP Snooping switch.
- Because Host A and Host B are members of the same multicast group, the switch does not notify the IP IGMP routing device (IGMP Querier) when Host A leaves the group, because the group still has another member Host B remaining. When Host B also leaves the group, the switch forwards the leave message to the IP IGMP Querier.
- The addition of a static mrouter port is only required when there is no upstream IGMP querier or an upstream router does not send topology discovery or maintenance messages (like IGMP General Queries or OSPF Hello packets).
- In this example, the configuration of a static mrouter port on port1.0.6 is provided to illustrate the **ip igmp snooping mrouter** command. However, this command would probably not be necessary, since the switch should dynamically set port1.0.6 to be an mrouter port as it receives IGMP Queries arriving from the IGMP Querier attached to port1.0.6.
- In this example, it is not necessary to explicitly configure the switch to work with IGMPv2 or IGMPv3. When the IGMP version is not configured then the switch will work with both versions of IGMP.

Table 32-1: Configuring IGMP Snooping on Switch 1 and IGMP Querier on Switch 2

Step 1.	**Configure IGMP Snooping (Switch 1)**	
1.	`awplus#` `configure terminal`	Enter Global Configuration mode.
2.	`awplus(config)#` `ip igmp snooping`	Enable IGMP Snooping globally. Snooping is enabled by default. Use this command only if you have previously disabled it.
3.	`awplus(config)#` `interface vlan1`	Enter Interface Configuration mode for VLAN 1.
4.	`awplus(config-if)#` `ip igmp snooping mrouter interface port1.0.6`	Configure port1.0.6 as a multicast router port to the IGMP Querier.
5.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
Step 2.	**Validate the configuration**	
6.	`awplus#` `exit`	Return to Privileged Exec mode.
7.	`awplus#` `show ip igmp interface vlan1`	Display the state of IGMP Snooping for VLAN 1.
8.	`awplus#` `show ip igmp groups`	Display the multicast groups with receivers directly connected to the router.
9.	`awplus#` `show ip igmp snooping mrouter interface vlan1`	Display the multicast router ports, both static and dynamic, in VLAN 1.
Step 3.	**Configure IGMP Querier (Switch 2)**	
1.	`awplus#` `configure terminal`	Enter Global Configuration mode.
2.	`awplus(config)#` `interface vlan1`	Enter Interface Configuration mode for VLAN 1.
3.	`awplus(config-if)#` `ip igmp`	Enable IGMP on VLAN 1 and configure the switch as an IGMP Querier.
Step 4.	**Validate the configuration**	
4.	`awplus#` `exit`	Return to Privileged Exec mode.
5.	`awplus#` `show ip igmp interface vlan1`	Display the state of IGMP Querier for VLAN 1.

Table 32-1: Configuring IGMP Snooping on Switch 1 and IGMP Querier on Switch 2 (cont.)

6.	`awplus#`	
	`show running-config`	Display the current dynamic configuration of Switch 2.

Query Solicitation

Query Solicitation minimizes the loss of multicast data after a topology change on networks that use EPSR or spanning tree (STP, RSTP, or MSTP) for loop protection. Without Query Solicitation, when the underlying link layer topology changes, multicast data flow can stop for up to several minutes, depending on which port goes down and how much of the IGMP query interval remained at the time of the topology change. Query Solicitation greatly reduces this disruption.

Query Solicitation operates without configuration in AlliedWare Plus™ switches running STP, RSTP, MSTP or EPSR. However, you may find it useful to manually enable Query Solicitation in loop-free networks running IGMP (see **Speeding up IGMP Convergence in a Non-Looped Topology**) and networks where not all switches support Query Solicitation (see **Enabling Query Solicitation on Multiple Switches in a Looped Topology**).

How Query Solicitation Works

Query Solicitation monitors STP, RSTP, MSTP and EPSR messages for topology changes. When it detects a change, it generates a special IGMP Leave message called a Query Solicit. The switch floods the Query Solicit message to all ports in every VLAN that Query Solicitation is enabled on. When the Querier receives the Query Solicit message, it sends out a General Query and waits for clients to respond with Membership Reports. These Reports update the snooping information throughout the network.

Query Solicit messages have a group address of 0.0.0.0.

Query Solicitation works by default (without you enabling it) on all VLANs on the root bridge in an STP instance and on all data VLANs on the master node in an EPSR instance. By default, the root bridge or master node always sends a Query Solicit message when any of the following events occur:

- an STP BPDU packet with the Topology Change (TC) flag arrives at the root bridge
- an STP port on a switch goes from a Discarding to Forwarding state
- the FDB gets flushed by EPSR

Query Solicitation Operation

When IGMP Snooping is enabled and EPSR or Spanning Tree changes the underlying link layer topology, this can interrupt multicast data flow for a significant length of time. This is because there is no way for switches in a network with interested clients to know where the traffic is available, due to the change in network topology. This change in network topology may take up to two IGMP Query intervals from the IGMP Querier, until the switches will know where to forward membership reports received by client hosts. During this time, those hosts will not receive multicast traffic.

Query solicitation prevents this by monitoring for any topology changes. When it detects a change, it generates a special IGMP Leave message known as a Query Solicit, and floods the Query Solicit message to all ports in every VLAN that query solicitation is enabled on. When the IGMP Querier receives the message, it responds by sending a General Query, which all IGMP listeners respond to. This refreshes snooped group membership information in the network.

Query solicitation reduces downtime to a negligible amount by triggering on topology changes. The generation of query solicitation messages in the network causes the IGMP Querier to send an IGMP Query immediately following a topology change. This enables the switches to know where to look for the traffic and thus to send reports to the correct switch upstream. This allows the multicast data traffic to be recovered instantly.

Query solicitation functions by default (without you enabling it) on all VLANs on the root bridge in an STP instance and on all data VLANs on the master node in an EPSR instance. By default, the root bridge or master node always sends a Query Solicit message when the topology changes.

If you have multiple STP or EPSR instances, query solicitation only sends Query Solicit messages on VLANs in the instance that experienced a topology change.

In switches other than the STP root bridge or EPSR master node, query solicitation is disabled by default, but you can enable it by using the **ip igmp snooping tcn query solicit** command.

If you enable query solicitation on a switch other than the STP root bridge or EPSR master node, both that switch and the root or master send a Query Solicit message.

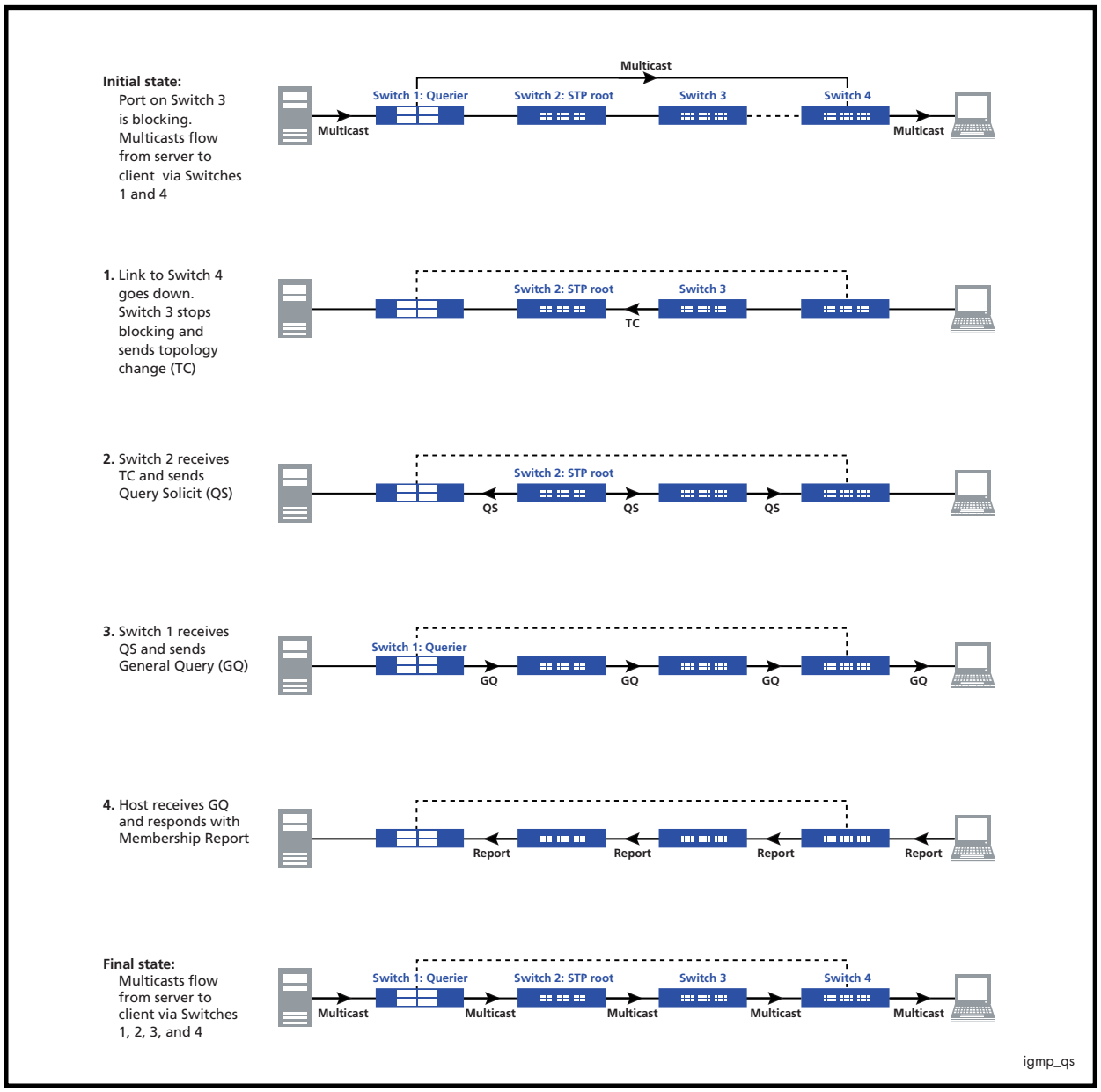
Once the Querier receives the Query Solicit message, it sends out a General Query and waits for responses, which update the snooping information throughout the network.

On switches other than the STP root bridge or the EPSR master node, you can disable query solicitation by using the no variant of the **ip igmp snooping tcn query solicit** command. In addition, on all switches, you can disable query solicitation on a per-vlan basis using the no variant of the **ip igmp snooping tcn query solicit** command in Interface Configuration mode, after specifying a VLAN first in Interface Configuration mode.

To see whether query solicitation is on or off, check the Query Solicitation field in output of the **show ip igmp interface** command. You can view running and startup configurations with **show running-config** and **show startup-config** commands to see if Query Solicitation is enabled.

The following figure shows how Query Solicitation works when a port goes down.

Figure 32-3: Query Solicitation when a port goes down



Speeding up IGMP Convergence in a Non-Looped Topology

For loop-free networks running IGMP, where it may take up to two minutes for multicasting to recover in a non-looped topology after a port comes back up, you can speed up convergence by enabling RSTP using the **spanning-tree mode** and **spanning-tree enable** commands.

RSTP enables the network to use Query Solicitation by default, and means that multicasting should resume within seconds, not minutes, of the link coming up.

Enabling Query Solicitation on Multiple Switches in a Looped Topology

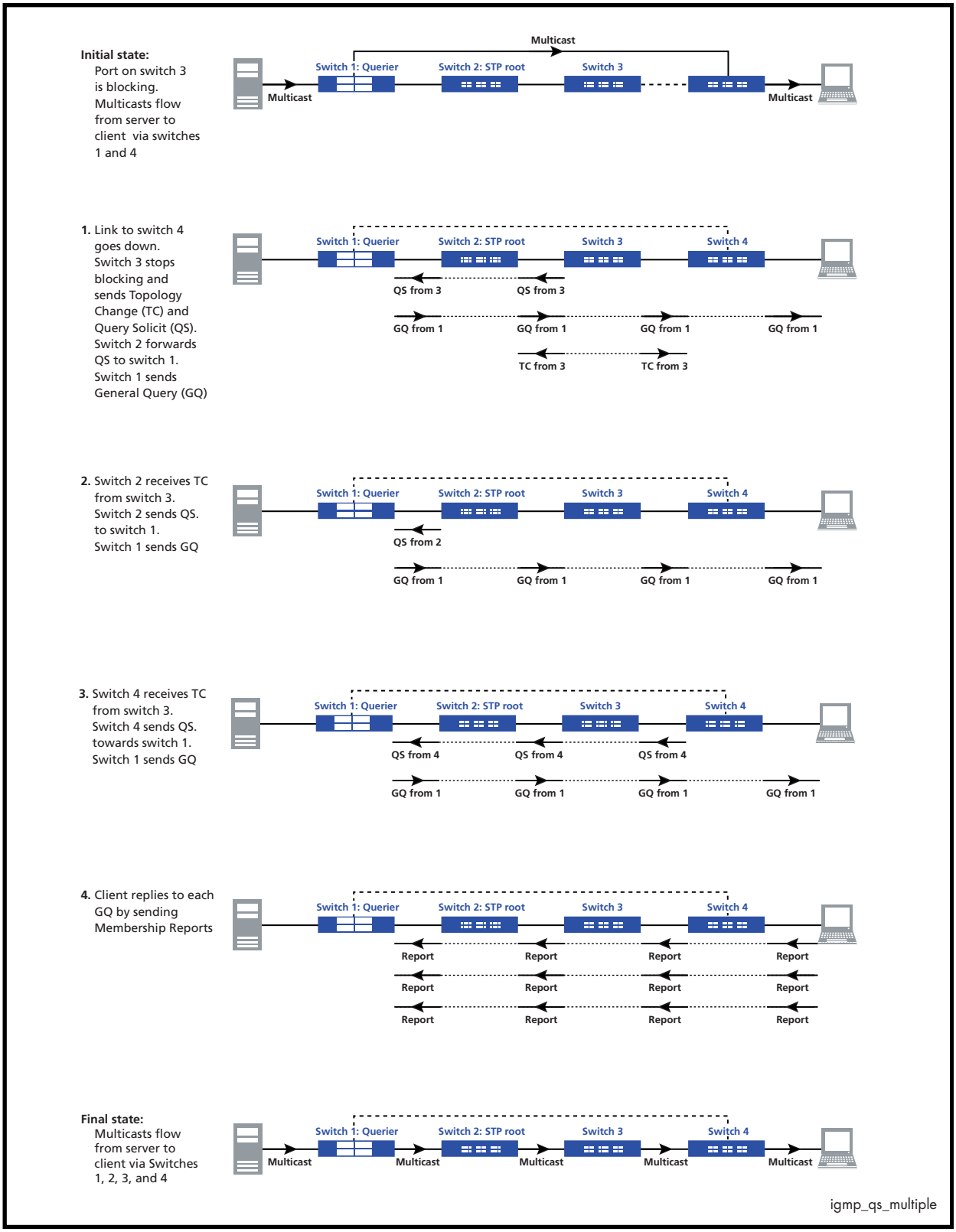
On networks that use spanning tree or EPSR, Query Solicitation is not normally required on switches other than the STP root bridge or EPSR master node. Therefore, it is only enabled by default on the root bridge and the master node.

However, in some networks you may need to turn on Query Solicitation on all switches - for example, if the network includes other switches that do not support Query Solicitation and therefore the STP root bridge may be a switch that does not send Query Solicit messages. To enable Query Solicitation, use the **ip igmp snooping tcn query solicit** command.

Every switch that has Query Solicitation enabled sends a Query Solicit message when it detects a topology change. Enabling it on multiple switches means you get multiple messages, but has no other disadvantage.

The following figure shows the packet flow for a four-switch network with Query Solicitation enabled on all the switches.

Figure 32-4: Packet flow for a four switch network with Query Solicitation enabled



Chapter 33: IGMP Snooping Commands

Introduction 33.2
Command List 33.2
clear ip igmp 33.2
clear ip igmp group 33.3
clear ip igmp interface 33.4
debug igmp 33.5
ip igmp snooping 33.6
ip igmp snooping fast-leave 33.7
ip igmp snooping querier 33.8
ip igmp snooping report-suppression 33.9
ip igmp snooping tcn query solicit 33.10
ip igmp static-group 33.12
ip igmp version 33.13
show debugging igmp 33.14
show ip igmp groups 33.15
show ip igmp interface 33.16
show ip igmp snooping statistics 33.19
undebug igmp 33.20

Introduction

The Internet Group Management Protocol (IGMP) module includes IGMP Snooping functionality. Some of the following commands may have commonalities and restrictions. These are described under the Usage section for each command.

Command List

This chapter provides an alphabetical reference of configure, clear, and show commands related to IGMP Snooping.

clear ip igmp

Use this command to clear all IGMP group membership records on all VLAN interfaces.

Syntax `clear ip igmp`

Mode Privileged Exec

Usage This command applies to VLAN interfaces configured for IGMP Snooping.

Example

```
awplus# clear ip igmp
```

Validation Commands **show ip igmp interface**
show running-config

Related Commands **clear ip igmp group**
clear ip igmp interface

clear ip igmp group

Use this command to clear IGMP group membership records for a specific group on either all VLAN interfaces, a single VLAN interface, or for a range of VLAN interfaces.

Syntax

```
clear ip igmp group *
clear ip igmp group <ip-address> <interface>
```

Parameter	Description
*	Clears all groups on all VLAN interfaces. This is an alias to the **clear ip igmp** command.
<ip-address>	Specifies the group whose membership records will be cleared from all VLAN interfaces, entered in the form A.B.C.D.
<interface>	Specifies the name of the VLAN interface; all groups learned on this VLAN interface are deleted.

Mode

Privileged Exec

Usage

This command applies to groups learned by IGMP Snooping.

In addition to the group a VLAN interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

Examples

```
awplus# clear ip igmp group *
awplus# clear ip igmp group 224.1.1.1 vlan1
```

Validation Commands

show ip igmp interface
show running-config

Related Commands

clear ip igmp
clear ip igmp interface

clear ip igmp interface

Use this command to clear IGMP group membership records on a particular VLAN interface.

Syntax `clear ip igmp interface <interface>`

Parameter	Description
<interface>	Specifies the name of the VLAN interface. All groups learned on this VLAN interface are deleted.

Mode Privileged Exec

Usage This command applies to interfaces configured for IGMP Snooping.

Example

```
awplus# clear ip igmp interface vlan1
```

Validation Commands **show ip igmp interface**
show running-config

Related Commands **clear ip igmp**
clear ip igmp group

debug igmp

Use this command to enable debugging of either all IGMP or a specific component of IGMP.

Use the **no** variant of this command to disable all IGMP debugging, or debugging of a specific component of IGMP.

Syntax

```
debug igmp {all|decode|encode|events|fsm|tib}
no debug igmp {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Enable or disable all debug options for IGMP
`decode`	Debug of IGMP packets that have been received
`encode`	Debug of IGMP packets that have been sent
`events`	Debug IGMP events
`fsm`	Debug IGMP Finite State Machine (FSM)
`tib`	Debug IGMP Tree Information Base (TIB)

Modes

Privileged Exec and Global Configuration

Usage

This command applies to interfaces configured for IGMP Snooping.

Example

```
awplus# configure terminal
awplus(config)# debug igmp all
```

Related Commands

show debugging igmp
undebug igmp

ip igmp snooping

Use this command to enable IGMP Snooping. When this command is used in the Global Configuration mode, IGMP Snooping is enabled at the switch level. When this command is used in Interface Configuration mode, IGMP Snooping is enabled for the specified VLANs.

Use the **no** variant of this command to either globally disable IGMP Snooping, or disable IGMP Snooping on a specified interface.

Note IGMP snooping cannot be disabled on an interface if IGMP snooping has already been disabled globally. IGMP snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.

Syntax

```
ip igmp snooping
no ip igmp snooping
```

Default By default, IGMP Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage For IGMP snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default.)

Both IGMP snooping and MLD snooping must be enabled globally on the switch for IGMP snooping to operate. MLD snooping is also enabled by default. To enable it if it has been disabled, use the **ipv6 mld snooping** command on page 35.8 in Global Configuration mode.

Ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Examples

```
awplus# configure terminal
awplus(config)# ip igmp snooping

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping
```

Related Commands

ipv6 mld snooping
show ip igmp interface
show running-config

ip igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing. The IGMP group-membership entry is removed as soon as an IGMP leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

Default IGMP Snooping fast-leave processing is disabled.

Mode Interface Configuration for a VLAN interface.

Usage This IGMP Snooping command can only be configured on VLAN interfaces.

Ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Example This example shows how to enable fast-leave processing on the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping fast-leave
```

Validation Commands

show ip igmp interface
show running-config

ip igmp snooping querier

Use this command to enable IGMP querier operation when no multicast routing protocol is configured. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to disable IGMP querier configuration.

Syntax

```
ip igmp snooping querier
no ip igmp snooping querier
```

Mode Interface Configuration for a VLAN interface.

Usage The IGMP Snooping querier uses the `0.0.0.0` Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

If an IP address is assigned to a VLAN, which has IGMP querier enabled on it, then the IGMP Snooping querier uses the VLAN's IP address as the Source IP Address in IGMP queries.

The IGMP Snooping Querier will not stop sending IGMP Queries if there is another IGMP Snooping Querier in the network with a lower Source IP Address.

Ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Note

Do not enable the IGMP Snooping Querier feature on a Layer 2 switch when there is an operational IGMP Querier in the network.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping querier
```

Validation Commands **show ip igmp interface**
show running-config

ip igmp snooping report-suppression

Use this command to enable report suppression for IGMP versions 1 and 2. This command applies to interfaces configured for IGMP Snooping.

Report suppression stops reports being sent to an upstream multicast router port when there are already downstream ports for this group on this interface.

Use the **no** variant of this command to disable report suppression.

Syntax

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Default Report suppression does not apply to IGMPv3, and is turned on by default for IGMPv1 and IGMPv2 reports.

Mode Interface Configuration for a VLAN interface.

Usage Ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Example This example shows how to enable report suppression for IGMPv2 reports for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
awplus(config-if)# ip igmp snooping report-suppression
```

Validation Commands **show ip igmp interface**
show running-config

ip igmp snooping tcn query solicit

Use this command to enable IGMP (Internet Group Management Protocol) Snooping TCN (Topology Change Notification) Query Solicitation feature. When this command is used in the Global Configuration mode, Query Solicitation is enabled.

Use the **no** variant of this command to disable IGMP Snooping TCN Query Solicitation. When the no variant of this command is used in Interface Configuration mode, this overrides the Global Configuration mode setting and Query Solicitation is disabled.

Syntax

```
ip igmp snooping tcn query solicit
no ip igmp snooping tcn query solicit
```

Default IGMP Snooping TCN Query Solicitation is disabled by default on the switch, unless the switch is the Master Node in an EPSR ring, or is the Root Bridge in a Spanning Tree.

When the switch is the Master Node in an EPSR ring, or the switch is the Root Bridge in a Spanning Tree, then IGMP Snooping TCN Query Solicitation is enabled by default and cannot be disabled using the Global Configuration mode command. However, Query Solicitation can be disabled for specified VLANs using this command from the Interface Configuration mode. Select the VLAN you want to disable in Interface Configuration mode then issue the no variant of this command to disable the specified VLAN without disabling this feature for other VLANs.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage Once enabled, if the switch is not an IGMP Querier, on detecting a topology change, the switch generates IGMP Query Solicit messages that are sent to all the ports of the vlan configured for IGMP Snooping on the switch.

On a switch that is not the Master Node in an EPSR ring or the Root Bridge in a Spanning Tree, Query Solicitation can be disabled using the **no** variant of this command after being enabled.

If the switch that detects a topology change is an IGMP Querier then the switch will generate an IGMP Query message.

Note that the **no** variant of this command when issued in Global Configuration mode has no effect on a switch that is the Master Node in an EPSR ring or on a switch that is a Root Bridge in a Spanning Tree. Query Solicitation is not disabled for the switch these instances. However, Query Solicitation can be disabled on a per-vlan basis from the Interface Configuration mode.

See the below state table that shows when Query Solicit messages are sent in these instances:

Command issued from Global Configuration	Switch is STP Root Bridge or the EPSR Master Node	Command issued from Interface Configuration	IGMP Query Solicit message sent on VLAN
No	Yes	Yes	Yes
Yes	Yes	No	No
Yes	Yes	Yes	Yes

See **"Query Solicitation" on page 32.9** for introductory information about the Query Solicitation feature.

To ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Examples

This example shows how to enable IGMP Snooping TCN Query Solicitation on a switch:

```
awplus# configure terminal
awplus(config)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation on a switch:

```
awplus# configure terminal
awplus(config)# no ip igmp snooping tcn query solicit
```

This example shows how to enable IGMP Snooping TCN Query Solicitation for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp snooping tcn query solicit
```

Validation Commands

show ip igmp interface
show running-config

ip igmp static-group

Use this command to statically configure multicast group membership entries on a VLAN interface, or to statically forward a multicast channel out a particular port or port range.

To statically add only a group membership, do not specify any parameters.

To statically add a (*,g) entry to forward a channel out of a port, specify only the multicast group address and the switch port range.

To statically add an (s,g) entry to forward a channel out of a port, specify the multicast group address, the source IP address, and the switch port range.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ip igmp static-group <ip-address> [source {<ip-source-addr>}]
    [interface <port>]

no ip igmp static-group <ip-address> [source {<ip-source-addr>}]
    [interface <port>]
```

Parameter	Description
<ip-address>	Standard IP Multicast group address, entered in the form A.B.C.D, to be configured as a static group member.
`source`	Optional.
<ip-source-addr>	Standard IP source address, entered in the form A.B.C.D, to be configured as a static source from where multicast packets originate.
`interface`	Use this parameter to specify a specific switch port or switch port range to statically forward the multicast group out of. If not used, static configuration is applied on all ports in the VLAN.
<port>	The port or port range to statically forward the group out of. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Interface Configuration for a VLAN interface.

Usage This command applies to IGMP Snooping on a VLAN interface, to statically add group and/or source records.

To ensure your VLAN is configured first, see **Chapter 16, Configuring VLANs**.

Example The following example show how to statically add group and source records for IGMP on the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp
awplus(config-if)# ip igmp static-group 226.1.2.4 source
10.2.3.4
```

ip igmp version

Use this command to set the current IGMP version (IGMP version 1, 2 or 3) on an interface.

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

Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameter	Description
<1-3>	IGMP protocol version number

Default The default IGMP protocol version number is 3.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to VLAN interfaces configured for IGMP.

Ensure your VLAN is configured first: see **Chapter 16, Configuring VLANs**.

Example

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip igmp version 2
```

Validation Commands **show ip igmp interface**

show debugging igmp

Use this command to display the IGMP debugging options set.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging igmp`

Mode User Exec and Privileged Exec

Example To display the IGMP debugging options set, enter the command:

```
awplus# show debugging igmp
```

Output **Figure 33-1: Example output from the show debugging igmp command**

```
IGMP Debugging status:
  IGMP Decoder debugging is on
  IGMP Encoder debugging is on
  IGMP Events debugging is on
  IGMP FSM debugging is on
  IGMP Tree-Info-Base (TIB) debugging is on
```

Related Commands **debug igmp**

show ip igmp groups

Use this command to display the multicast groups with receivers directly connected to the router, and learned through IGMP.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip igmp groups [<ip-address>|<interface> detail]`

Parameter	Description
<ip-address>	Address of the multicast group, entered in the form A.B.C.D.
<interface>	Interface name for which to display local information.

Mode User Exec and Privileged Exec

Example The following command displays local-membership information for all ports in all interfaces:

```
awplus# show ip igmp groups
```

Output **Figure 33-2: Example output from the show ip igmp groups command**

```
IGMP Connected Group Membership
Group Address    Interface       Uptime    Expires   Last
Reporter
224.0.1.1        port1.0.1       00:00:09  00:04:17  10.10.0.82
224.0.1.24       port1.0.2       00:00:06  00:04:14  10.10.0.84
224.0.1.40       port1.0.3       00:00:09  00:04:15  10.10.0.91
224.0.1.60       port1.0.3       00:00:05  00:04:15  10.10.0.7
224.100.100.100  port1.0.1       00:00:11  00:04:13  10.10.0.91
228.5.16.8       port1.0.3       00:00:11  00:04:16  10.10.0.91
228.81.16.8      port1.0.7       00:00:05  00:04:15  10.10.0.91
228.249.13.8     port1.0.3       00:00:08  00:04:17  10.10.0.91
235.80.68.83     port1.0.11      00:00:12  00:04:15  10.10.0.40
239.255.255.250  port1.0.3       00:00:12  00:04:15  10.10.0.228
239.255.255.254  port1.0.12      00:00:08  00:04:13  10.10.0.84
```

Table 33-1: Parameters in the output of the show ip igmp groups command

Parameter	Description
`Group Address`	Address of the multicast group.
`Interface`	Port through which the group is reachable.
`Uptime`	The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device.
`Expires`	Time (in hours, minutes, and seconds) until the entry expires.
`Last Reporter`	Last host to report being a member of the multicast group.

show ip igmp interface

Use this command to display the state of IGMP Snooping for a specified VLAN, or all VLANs. IGMP is shown as Active or Disabled in the show output.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip igmp interface [<interface>]`

Parameter	Description
<interface>	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Examples The following output shows IGMP interface status for **vlan2** (with IGMP Snooping enabled):

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

The following output shows IGMP interface status for **vlan2** (with IGMP Snooping disabled):

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#no ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is not enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

The following command displays the IGMP interface status and Query Solicitation for **vlan3**:

```
awplus#show ip igmp interface vlan3
Interface vlan3 (Index 203)
 IGMP Enabled, Active, Querier, Version 3 (default)
 Internet address is 192.168.9.1
 IGMP interface has 256 group-record states
 IGMP activity: 51840 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 250 seconds
 IGMP max query response time is 1 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 251 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally enabled
  Num. query-solicit packets: 1 sent, 10 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

Note

Query Solicitation status information is highlighted in **bold** in the above output.

Use the **show ip igmp interface** command to validate that Query Solicitation is enabled and to show the number of query-solicit message packets sent and received on a VLAN.

Related Commands

clear ip igmp
clear ip igmp group
clear ip igmp interface
ip igmp snooping
ip igmp snooping fast-leave
ip igmp snooping querier
ip igmp snooping report-suppression
ip igmp snooping tcn query solicit
ip igmp version

show ip igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ip igmp snooping statistics interface <interface-range>
   [group [<ip-address>]]
```

Parameter	Description
<ip-address>	Optionally specify the address of the multicast group, entered in the form A.B.C.D.
<interface>	Specify the name of the VLAN interface or interface range.

Mode User Exec and Privileged Exec

Example To display IGMP statistical information for **vlan1** and **vlan2**, use the command:

```
awplus# show ip igmp snooping statistics interface
        vlan1-vlan2
```

Output **Figure 33-3: Example output from the show ip igmp snooping statistics command**

```
IGMP Snooping statistics for vlan1
Interface:      port1.0.3
Group:          224.1.1.1
Uptime:         00:00:09
Group mode:     Exclude (Expires: 00:04:10)
Last reporter:  10.4.4.5
Source list is empty
IGMP Snooping statistics for vlan2
Interface:      port1.0.4
Group:          224.1.1.2
Uptime:         00:00:19
Group mode:     Exclude (Expires: 00:05:10)
Last reporter:  10.4.4.6
Source list is empty
```

undebug igmp

This command applies the functionality of the no **debug igmp** command on page 33.5.

Chapter 34: MLD Snooping Introduction and Configuration

Introduction 34.2
MLD Snooping 34.2

Introduction

Multicast Listener Discovery (MLD) is used to exchange membership status information between IPv6 routers that support multicasting and members of multicast groups on a network segment. Host membership in a multicast group is reported by individual member hosts, and membership status is periodically polled by multicast routers.

MLD Snooping

MLD Snooping is a feature whereby a Layer 2 device listens to or "snoops" the MLD messages passing through the device or from member hosts and multicast routers. The purpose of MLD Snooping is to provide efficient Layer 2 multicast forwarding, by sending only to hosts that have expressed an interest in receiving the multicast data.

Hosts express an interest in receiving multicast data for a given multicast group by sending an MLD join message. Without MLD Snooping, if one host expresses an interest in getting multicast data for a given group, by sending an MLD join for the multicast group, then all hosts connected to the same VLAN will also receive the multicast data. This wastes bandwidth on the device ports connected to the host that are not interested in receiving the multicast data. Snooping takes note of exactly which ports have received joins for a given group, and send that group only to those ports.

MLD Snooping is enabled by default globally for the device. It can be enabled and disabled on a per-VLAN basis.

MLD Snooping makes a distinction between Member ports, which are ports connected to members hosts, and Router ports, which are ports connected to, or directed towards, a Layer 3 router or a Layer 3 device.

Figure 34-1: Sample running-config showing an MLD Snooping Querier set on vlan2

```
!
ipv6 mld snooping
!
interface vlan2
  ipv6 mld snooping querier
!
```

For detailed information about the commands used to configure MLD Snooping, see **Chapter 34, MLD Snooping Introduction and Configuration**.

The following examples configure MLD Snooping:

- **Enabling MLD Snooping globally and on an interface**
- **Configuring a Multicast Router statically on an interface**
- **Enabling MLD Snooping Fast-Leave Processing on an interface**
- **Configuring MLD Snooping Report Suppression on an interface**
- **Enabling the MLD Snooping Querier on an interface**

Enabling MLD Snooping globally and on an interface

To globally enable and show MLD Snooping on the device, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
awplus(config)# exit
awplus# show ipv6 mld interface
```

Note that entering `show ipv6 mld interface` without an optional interface parameter displays MLD information for all configured interfaces globally on the device.

To enable and show MLD Snooping on VLAN interface `vlan2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note that entering `show ipv6 mld interface vlan2` with the optional interface parameter displays MLD information for that specified configured interface on the device.

Configuring a Multicast Router statically on an interface

To configure and show a static connection to a Multicast Router for VLAN interface `vlan2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface
                   port1.0.2
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note the VLAN interface to the Multicast Router must be administratively up and the line protocol must be up to configure a static connection to a Multicast Router on the VLAN.

Enabling MLD Snooping Fast-Leave Processing on an interface

To enable and show MLD Snooping Fast-Leave Processing on VLAN interface `vlan2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Configuring MLD Snooping Report Suppression on an interface

To enable and show MLD Snooping Report Suppression on VLAN interface `vlan2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Enabling the MLD Snooping Querier on an interface

Use the MLD Snooping Querier to support MLD Snooping in a VLAN where PIM-SMv6 and MLD are not configured and whenever you do not need to route IPv6 multicast traffic.

You can configure the device to generate MLD queries on a VLAN interface if multicast routing is not enabled. For each VLAN that is connected to devicees that use MLD Snooping to report multicast traffic, configure one device as the MLD Snooping Querier.

To enable and show MLD Snooping Querier on VLAN interface `vlan2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping querier
awplus(config-if)# exit
awplus(config)# exit
awplus# show ipv6 mld interface vlan2
```

Note that the MLD Snooping Querier is configured in Interface Configuration mode only. You cannot configure MLD Snooping Querier globally for all VLAN interfaces on a device.

Chapter 35: MLD Snooping Commands

Command List 35.2
clear ipv6 mld 35.2
clear ipv6 mld group 35.3
clear ipv6 mld interface 35.3
debug mld 35.4
ipv6 mld access-group 35.5
ipv6 mld limit 35.6
ipv6 mld snooping 35.8
ipv6 mld snooping fast-leave 35.10
ipv6 mld snooping mrouter 35.11
ipv6 mld snooping querier 35.13
ipv6 mld snooping report-suppression 35.14
ipv6 mld static-group 35.16
show debugging mld 35.19
show ipv6 mld groups 35.20
show ipv6 mld interface 35.21
show ipv6 mld snooping mrouter 35.22
show ipv6 mld snooping statistics 35.23

Command List

This chapter provides an alphabetical reference of configuration, clear, and show commands related to MLD Snooping.

clear ipv6 mld

Use this command to clear all MLD local memberships on all interfaces.

Syntax

```
clear ipv6 mld
```

Mode

Privileged Exec

Example

```
awplus# clear ipv6 mld
```

Related Commands

clear ipv6 mld group
clear ipv6 mld interface

clear ipv6 mld group

Use this command to clear MLD specific local-membership(s) on all interfaces, for a particular group.

Syntax

```
clear ipv6 mld group {*|<ipv6-address>}
```

Parameter	Description
*	Clears all groups on all interfaces. This is an alias to the **clear ipv6 mld** command.
<ipv6-address>	Specify the group address for which MLD local-memberships are to be cleared from all interfaces. Specify the IPv6 multicast group address in the format in the format X:X::X:X.

Mode

Privileged Exec

Example

```
awplus# clear ipv6 mld group *
```

Related Commands

clear ipv6 mld
clear ipv6 mld interface

clear ipv6 mld interface

Use this command to clear MLD interface entries.

Syntax

```
clear ipv6 mld interface <interface>
```

Parameter	Description
<interface>	Specifies name of the interface; all groups learned from this interface are deleted.

Mode

Privileged Exec

Example

```
awplus# clear ipv6 mld interface vlan2
```

Related Commands

clear ipv6 mld
clear ipv6 mld group

debug mld

Use this command to enable all MLD debugging modes, or a specific MLD debugging mode.

Use the **no** variant of this command to disable all MLD debugging modes, or a specific MLD debugging mode.

Syntax

```
debug mld {all|decode|encode|events|fsm|tib}
no debug mld {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Debug all MLD.
`decode`	Debug MLD decoding.
`encode`	Debug MLD encoding.
`events`	Debug MLD events.
`fsm`	Debug MLD Finite State Machine (FSM).
`tib`	Debug MLD Tree Information Base (TIB).

Mode Privileged Exec and Global Configuration

Examples

```
awplus# configure terminal
awplus(config)# debug mld all

awplus# configure terminal
awplus(config)# debug mld decode

awplus# configure terminal
awplus(config)# debug mld encode

awplus# configure terminal
awplus(config)# debug mld events
```

Related Commands show debugging mld

ipv6 mld access-group

Use this command to control the multicast local-membership groups learned on an interface.

Use the **no** variant of this command to disable this access control.

Syntax

```
ipv6 mld access-group <IPv6-access-list-name>
no ipv6 mld access-group
```

Parameter	Description
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name. See **Chapter 39, IPv6 Software Access Control List (ACL) Commands** for supported IPv6 ACLs.

Default No access list is configured by default.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Examples In the following example, the VLAN interface `vlan2` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

In the following example, the VLAN interfaces `vlan2-vlan4` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

ipv6 mld limit

Use this command to configure a limit on the maximum number of group memberships that may be learned. The limit may be set for the device as a whole, or for a specific interface.

Once the specified group membership limit is reached, all further local-memberships will be ignored.

Optionally, an exception access-list can be configured to specify the group-address(es) that are exempted from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

Syntax

```
ipv6 mld limit <limitvalue> [except <IPv6-access-list-name>]
no ipv6 mld limit
```

Parameter	Description
<limitvalue>	<2-512> Maximum number of group membership states.
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups, which are exempted from being subject to the configured limit. See **Chapter 39, IPv6 Software Access Control List (ACL) Commands** for supported IPv6 ACLs.

Default The default limit, which is reset by the **no** variant of this command, is the same as maximum number of group membership entries that can be learned with the **ipv6 mld limit** command.

The default limit of group membership entries that can be learned is 512 entries.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Examples The following example configures an MLD limit of 100 group-memberships across all VLAN interfaces on which MLD is enabled, and excludes groups in the range `ff1e:0db8:0001::/64` from this limitation:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard v6grp permit
ff1e:0db8:0001::/64
awplus(config)# ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

Related Commands **show ipv6 mld groups**

ipv6 mld snooping

Use this command to enable MLD Snooping. When this command is issued in the Global Configuration mode, MLD Snooping is enabled globally for the device. When this command is issued in Interface mode for a VLAN then MLD Snooping is enabled for the specified VLAN. Note that MLD Snooping is enabled on the VLAN only if it is enabled globally and on the VLAN.

Use the **no** variant of this command to globally disable MLD Snooping in Global Configuration mode, or for the specified VLAN interface in Interface mode.

Syntax

```
ipv6 mld snooping
no ipv6 mld snooping
```

Default By default, MLD Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage For MLD Snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default).

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

Examples To configure MLD Snooping on the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
```

To configure MLD Snooping on the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# no ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config)# no ipv6 mld snooping
```

To configure MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
```

To disable MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 mld snooping
```

ipv6 mld snooping fast-leave

Use this command to enable MLD Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the MLD group-membership is removed as soon as an MLD leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax

```
ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave
```

Default MLD Snooping fast-leave processing is disabled.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command can only be configured on VLAN interfaces.

Examples This example shows how to enable fast-leave processing on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
```

This example shows how to enable fast-leave processing on the VLAN interface `vlan2-vlan4`.

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping fast-leave
```

ipv6 mld snooping mrouter

Use this command to statically configure the specified port as a Multicast Router interface for MLD Snooping within the specified VLAN.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to remove the static configuration of the interface as a Multicast Router interface.

Syntax

```
ipv6 mld snooping mrouter interface <port>
no ipv6 mld snooping mrouter interface <port>
```

Parameter	Description
<port>	Specify the name of the port.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command statically configures a device port as a Multicast Router interface.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if `port1.0.1` and `port1.0.6` are ports on an EPSR data VLAN `vlan101`, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

Output **Figure 35-1: Example ipv6 mld snooping mrouter commands when static IPv6 multicast routing is being used and the destination VLAN is an ESPR data VLAN:**

```
awplus>enable
awplus#configure terminal
awplus(config)#interface vlan101
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.6
```

Examples This example shows how to specify the next-hop interface to the multicast router for VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

This example shows how to specify the next-hop interface to the multicast router for VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

ipv6 mld snooping querier

Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD Snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

Use the **no** variant of this command to disable MLD querier configuration.

Syntax

```
ipv6 mld snooping querier
no ipv6 mld snooping querier
```

Mode Interface Configuration for a specified VLAN interface.

Usage This command can only be configured on a single VLAN interface - not on multiple VLANs.

The MLD Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as an MLD querier for faster network convergence.

The MLD Snooping querier does not start, or automatically cease, the MLD Querier operation if it detects query message(s) from a multicast router. It restarts as an MLD Snooping querier if no queries are seen within the other querier interval.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping querier
```

ipv6 mld snooping report-suppression

Use this command to enable report suppression from hosts for Multicast Listener Discovery version 1 (MLDv1) on a VLAN in Interface Configuration mode.

Use the **no** variant of this command to disable report suppression on a VLAN in Interface Configuration mode.

Syntax

```
ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression
```

Default Report suppression does not apply to MLDv2, and is turned on by default for MLDv1 reports.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command can only be configured on VLAN interfaces.

MLDv1 Snooping maybe configured to suppress reports from hosts. When a querier sends a query, only the first report for particular set of group(s) from a host will be forwarded to the querier by the MLD Snooping device. Similar reports (to the same set of groups) from other hosts, which would not change group memberships in the querier, will be suppressed by the MLD Snooping device to prevent 'flooding' of query responses.

Examples This example shows how to enable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 mld snooping report-suppression
```

This example shows how to enable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ipv6 mld snooping report-suppression
```

ipv6 mld static-group

Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ipv6 mld static-group <ipv6-group-address>
    [source <ipv6-source-address>|ssm-map] [interface <port>]

no ipv6 mld static-group <ipv6-group-address>
    [source <ipv6-source-address>|ssm-map] [interface <port>]
```

Parameter	Description
<ipv6-group-address>	Specify a standard IPv6 Multicast group address to be configured as a static group member. The IPv6 address uses the format X:X::X:X.
<ipv6-source-address>	Optional. Specify a standard IPv6 source address to be configured as a static source from where multicast packets originate. The IPv6 address uses the format X:X::X:X.
`ssm-map`	Mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate these (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.
<port>	Optional. Physical interface. This parameter specifies a physical port. If this parameter is used, the static configuration is applied to just to that physical interface. If this parameter is not used, the static configuration is applied on all ports in the VLAN.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to MLD Snooping on a VLAN interface to statically add groups and/or source records.

Examples The following examples show how to statically add group and/or source records for MLD:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10

awplus # configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
                   fe80::2fd:6cff:fe1c:b
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map
```

The following examples show how to statically add group and/or source records for MLD Snooping on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 interface
port1.0.4
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b interface port1.0.4
```

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map interface port1.0.4
```

show debugging mld

Use this command to display the MLD debugging modes enabled with the **debug mld** command.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show debugging mld
```

Mode

Privileged Exec

Example

```
awplus# show debugging mld
```

Output

```
show debugging mld
MLD Debugging status:
  MLD Decoder debugging is on
  MLD Encoder debugging is on
  MLD Events debugging is on
  MLD FSM debugging is on
  MLD Tree-Info-Base (TIB) debugging is on
```

Related Commands

debug mld

show ipv6 mld groups

Use this command to display the multicast groups with receivers directly connected to the router, and learned through MLD.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 mld groups [<ipv6-address> |<interface>] [detail]
```

Parameter	Description
<ipv6-address>	Optional. Specify Address of the multicast group in format X:X::X:X.
<interface>	Optional. Specify the Interface name for which to display local information.

Mode

User Exec and Privileged Exec

Examples

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

Output

```
MLD Connected Group Membership

Group Address Interface  Uptime  Expires Last Reporter

ff08::1     port1.0.1 00:00:24 stopped fe80::eecd:6dff:fe6b:4783
```

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

Output

```
MLD Connected Group Membership Details for port1.0.1
Interface:      port1.0.1
Group:          ff08::1
Uptime:         00:00:13
Group mode:     Include ()
Last reporter:  fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static )
  Source Address                Uptime    v2 Exp    Fwd  Flags
  2001:db8::1                   00:00:13  00:04:07  Yes  R
  2002:db8::3                   00:00:13  00:04:07  Yes  R
```

show ipv6 mld interface

Use this command to display the state of MLD and MLD Snooping for a specified interface, or all interfaces.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 mld interface [<interface>]
```

Parameter	Description
<interface>	Interface name.

Mode

User Exec and Privileged Exec

Example

The following command displays MLD interface status on all interfaces enabled for MLD:

```
awplus# show ipv6 mld interface
```

Output

```
awplus#show ipv6 mld interface
Interface vlan1 (Index 301)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::215:77ff:fec9:7468
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD robustness variable is 2
 MLD last member query count is 2
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is enabled
 MLD Snooping report suppression is enabled
```

show ipv6 mld snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN. If you do not specify a VLAN interface then all the VLAN interfaces are displayed.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show ipv6 mld snooping mrouter [<interface>]
```

Parameter	Description
<interface>	Optional. Specify the name of the VLAN interface. Note: If you do not specify a single VLAN interface, then all VLAN interfaces are shown.

Mode User Exec and Privileged Exec

Examples The following command displays the multicast router interfaces in `vlan2`:

```
awplus# show ipv6 mld snooping mrouter vlan2
```

Output

```
awplus#show ipv6 mld snooping mrouter vlan2
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
```

The following command displays the multicast router interfaces for all VLAN interfaces:

```
awplus# show ipv6 mld snooping mrouter
```

Output

```
awplus#show ipv6 mld snooping mrouter
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
3       port1.0.4    Statically Assigned
3       port1.0.5    Statically Assigned
```

show ipv6 mld snooping statistics

Use this command to display MLD Snooping statistics data.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ipv6 mld snooping statistics interface <interface>`

Parameter	Description
<interface>	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Example The following command displays MLDv2 statistical information for `vlan1`:

```
awplus# show ipv6 mld snooping statistics interface vlan1
```

Output

```
awplus#show ipv6 mld snooping statistics interface vlan1
MLD Snooping statistics for vlan1
Interface:      port1.0.1
Group:          ff08::1
Uptime:         00:02:18
Group mode:     Include ()
Last reporter:  fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static )
  Source Address       Uptime    v2 Exp    Fwd  Flags
  2001:db8::1          00:02:18  00:02:02  Yes  R
  2001:db8::3          00:02:18  00:02:02  Yes  R
```

Part 5: Access and Security

- Chapter 36 Access Control Lists Introduction
- Chapter 37 IPv4 Hardware Access Control List (ACL) Commands
- Chapter 38 IPv4 Software Access Control List (ACL) Commands
- Chapter 39 IPv6 Software Access Control List (ACL) Commands
- Chapter 40 Quality of Service (QoS) Introduction
- Chapter 41 QoS Commands
- Chapter 42 Authentication Introduction and Configuration
- Chapter 43 Authentication Commands
- Chapter 44 AAA Introduction and Configuration
- Chapter 45 AAA Commands
- Chapter 46 802.1X Introduction and Configuration
- Chapter 47 802.1X Commands
- Chapter 48 RADIUS Introduction and Configuration
- Chapter 49 RADIUS Commands
- Chapter 50 TACACS+ Introduction and Configuration
- Chapter 51 TACACS+ Commands
- Chapter 52 Secure Shell (SSH) Introduction
- Chapter 53 Secure Shell (SSH) Configuration
- Chapter 54 Secure Shell (SSH) Commands

- Chapter 55 DHCP Snooping Introduction and Configuration
- Chapter 56 DHCP Snooping Commands

Chapter 36: Access Control Lists Introduction

Introduction 36.2
Overview 36.2
ACL Rules 36.3
ACL Source and Destination Addresses 36.3
ACL Reverse Masking 36.3
Hardware and Software ACL Types 36.4
Defining Hardware MAC ACLs 36.5
Defining Hardware IP ACLs 36.6
Actions for Hardware ACLs 36.7
Attaching Hardware ACLs to Interfaces 36.7
Hardware ACLs and QoS Classifications 36.8
Classifying Your Traffic 36.8
Security ACLs 36.8
QoS ACLs 36.9
Attaching Hardware ACLs Using QoS 36.9
Filtering Hardware ACLs with QoS 36.11
Using QoS Match Commands with TCP Flags 36.11
ACL Filter Sequence Numbers 36.14
ACL Filter Sequence Number Behavior 36.14
ACL Filter Sequence Number Applicability 36.14
ACL Filter Sequence Number Types 36.15
ACL Filter Sequence Configuration 36.18
Creating ACLs in Global Configuration Mode 36.20
Display the ACL configuration details 36.22

Introduction

This chapter describes Access Control Lists (ACLs), and general ACL configuration information.

See **Chapter 38, IPv4 Software Access Control List (ACL) Commands** and **Chapter 39, IPv6 Software Access Control List (ACL) Commands** for detailed command information and command examples about IPv4 and IPv6 software ACLs as applied to Routing and Multicasting.

See all relevant Routing commands and configurations in **"IP and IPv6"** and all relevant Multicast commands and configurations in **"Multicast Applications"**.

Overview

An Access Control List (ACL) is one filter, or a sequence of filters, that are applied to an interface to either block or pass (or when using QoS, apply priority to) packets that match the filter definitions. ACLs are used to restrict network access by hosts and devices and to limit network traffic.

An ACL contains an ordered list of filters. Each filter specifies either permit or deny and a set of conditions the packet must satisfy in order to match the filter. The meaning of permit or deny entries depends on the context in which the ACL is used - either on an inbound or an outbound interface.

When a packet is received on an interface, the switch compares fields in the packet against filters in the ACL to check whether the packet has permission to be forwarded, based on the filter properties. The first match determines whether the switch accepts or rejects the packets. If no entries match, the switch rejects the packets. If there are no restrictions, the switch forwards the packets.

Because filters in an ACL are applied sequentially and their action stops at the first match, it is very important that you apply the filters in the correct order. For example you might want to pass all traffic from VLAN 4 except for that arriving from two selected addresses A and B. Setting up a filter that first passes all traffic from VLAN 4 then denies traffic from addresses A and B will not filter out traffic from A and B if they are members VLAN 4. To ensure that the traffic from A and B is always blocked you should first apply the filter to block traffic from A and B, then apply the filter to allow all traffic from VLAN 4.

You can assign sequence numbers to filters. See **"ACL Filter Sequence Numbers" on page 36.14** for more information.

ACL Rules

- The source or destination address or the protocol of each packet being filtered are tested against the filters in the ACL, one condition at a time (for a permit or a deny filter).
- If a packet does not match a filter then the packet is checked against the next filter in the ACL.
- If a packet and a filter match, the subsequent filters in the ACL are not checked and the packet is permitted or denied as specified in the matched filter.
- The first filter that the packet matches determines whether the packet is permitted or denied. After the first match, no subsequent filters are considered.
- If the ACL denies the address or protocol then the software discards the packet.
- For software ACLs, if no filters match then the packet is dropped.
- For hardware ACLs, if no filters match then the packet is forwarded.
- Checking stops after the first match, so the order of the filters in the ACL is critical. The same permit or deny filter specified in a different order could result in a packet being passed in one situation and denied in another situation.
- One ACL per interface, per protocol, per direction is allowed. However, each ACL assigned per interface, per protocol, per direction may also have multiple filters.
- For inbound ACLs, a permit filter continues to process the packet after receiving it on an inbound interface, and a deny filter discards the packet.

ACL Source and Destination Addresses

Configure source addresses in ACL filters to filter packets coming **from** specified networking devices or hosts. Configure destination addresses in ACL filters to filter packets going **to** specified networking devices or hosts.

ACL Reverse Masking

ACLs uses reverse masking, also referred to as wildcard masking, to indicate to the switch whether to check or ignore corresponding IP address bits when comparing the address bits in an ACL filter to a packet being submitted to the ACL.

Reverse masking for IP address bits specify how the switch treats the corresponding IP address bits. A reverse mask is also called an inverted mask because a 1 and 0 mean the opposite of what they mean in a subnet or a network mask.

- A reverse mask bit 0 means check the corresponding bit value.
- A reverse mask bit 1 means ignore the corresponding bit value.

Hardware and Software ACL Types

Access Control Lists (ACLs) used in AlliedWare Plus™ are separated into two different types, **software ACLs** and **hardware ACLs**. You can define both types as either named or numbered.

Note

The filtering principles applied to software ACLs (those in the range 1 to 2699) are different to those applied to hardware ACLs (those in the range 3000 to 4699).
Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.
Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Numbered ACLs (for hardware and software ACLs)

Numbered ACLs are assigned an ACL number within the range 1 to 4699. ACL numbers are grouped into ranges, where each range denotes a specific functionality. The following table shows the number ranges and functionality that your switch supports.

Table 36-1: ACL numeric ranges and functionality

ACL Number Range	Function
1 to 99	IP standard ACL [1]
100 to 199	IP extended ACL [1]
1300 to 1999	IP standard expanded ACL [1]
2000 to 2699	IP extended expanded ACL [1]
3000 to 3699	Hardware IP ACL
4000 to 4699	Hardware MAC ACL

1. **Software ACLs that use either the ranges 1-99, 100-199, 1300-1999, 2000-2699, or are named ACLs (that use the standard or extended keyword followed by a text string), are used in features such as SNMP.**

Hardware ACLs

These ACL types are applied directly to an interface, or are used for QoS classifications. They use the following ranges:

- 3000-3699 for Hardware IP ACLs
- 4000-4699 for Hardware MAC ACLs
- named hardware IPv4 ACLs

Software ACLs

These ACLs types can be either named ACLs, using the standard or extended keyword followed by a text string, or they can use the following ranges:

- 1-99 (IP standard ACL range)
- 100-199 (IP extended ACL range)
- 1300-1999 (IP standard expanded ACL range)
- 2000-2699 (IP extended expanded ACL range)
- named standard IPv4 ACLs
- named extended IPv4 ACLs
- named standard IPv6 ACLs
- named extended IPv6 ACLs

Software ACLs are used in features such as SNMP.

See **Chapter 38, IPv4 Software Access Control List (ACL) Commands** and **Chapter 39, IPv6 Software Access Control List (ACL) Commands** for detailed command information and command examples about IPv4 and IPv6 software ACLs as applied to routing and multicasting. See all relevant Routing commands and configurations in **"IP and IPv6"** and all relevant multicast commands and configurations in **"Multicast Applications"**.

Defining Hardware MAC ACLs

These are used to filter traffic based on specific source or destination MAC addresses contained within the data frames. They can be applied to ports in the form of access groups.

A MAC access list requires the following components:

- an ACL number in the range 4000-4699
- an action, permit, or deny. See **"Actions for Hardware ACLs" on page 36.7**
- a source MAC address. You can use the format, HHHH.HHHH.HHHH to filter on a specific MAC address (where H is a hexadecimal number), or you can filter on any source MAC address by entering the word "any".
- a source MAC mask. This mask determines which portion of the source MAC address header will be compared with that found in the incoming packets. The mask is configured in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number. In practice each hex number will normally be either 0 (to represent a match) or F (to represent a don't care condition). A mask is not required if the source address is specified as "any".
- a destination MAC address. You can use the format, HHHH.HHHH.HHHH to filter on a specific MAC address (where H is a hexadecimal number), or you can filter on any destination MAC address by entering the word "any".
- a destination MAC mask. This mask determines which portion of the destination MAC address header will be compared with that found in the incoming packets. The mask is configured in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number. In practice each hex number will normally be either 0 (to represent a match) or F (to represent a don't care condition). A mask is not required if the source address is specified as "any".

Example To permit packets coming from a specific MAC address of 0030.841A.1234 and with any destination address:

```
awplus# configure terminal
awplus(config)# access-list 4000 permit 0030.841A.1234
0000.0000.0000 any
```

Defining Hardware IP ACLs

Hardware IP ACLs are used to filter traffic based on specific source or destination IP addresses contained within the data frames. They can be applied to ports in the form of access groups.

An IP access list requires the following components:

- an ACL number in the range 3000-3699
- an action, see **"Actions for Hardware ACLs" on page 36.7**
- a packet type:
  - « IP: This matches any type of IP packet. A source and destination address must be specified, although they can be "any".
  - « ICMP: This matches ICMP packets. A source and destination address must be specified, although they can be "any". An ICMP type can optionally be specified after the destination address.
  - « TCP: This matches TCP packets. A source and destination address must be specified, although they can be "any". After the source address, a source port can optionally be specified and after the destination address a destination port can optionally be specified. The port matching can be done using **eq** (equal to), **gt** (greater than), **lt** (less than), **ne** (not equal to), or **range** (for a range of ports, which requires a start port and an end port).
  - « UDP: This matches UDP packets and has the same options as TCP.
  - « proto: This allows any IP protocol type to be specified. A source and destination address must be also specified, although they can be "any".

For example, to match (and permit) any type of IP packet containing a destination address of 192.168.1.1

```
awplus(config)# access-list 3000 permit ip any 192.168.1.1/32
```

To match (and permit) an ICMP packet with a source address of 192.168.x.x and an ICMP code of 4

```
awplus(config)# access-list 3001 permit icmp 192.168.0.0/16
any icmp-type 4
```

To match a TCP packet with a source address of 192.168.x.x, source port of 80 and a destination port from 100 to 150:

```
awplus(config)# access-list 3002 permit tcp 192.168.0.0/16 eq
80 any range 100 150
```

To match a UDP packet with a source address of 192.168.x.x, a destination address of 192.168.1.x, and a destination port greater than 80:

```
awplus(config)# access-list 3003 permit udp 192.168.0.0/16
                192.168.1.0/24 gt 80
```

Note that an IP address mask can be specified using either of the following notations:

- "A.B.C.D/M": This is the most common; e.g. 192.168.1.0/24
- "A.B.C.D A.B.C.D": 192.168.1.1 0.0.0.0 is the same as 192.168.1.1/32 and 192.168.1.1 255.255.255.255 is the same as "any"
- "host A.B.C.D": This is the same as A.B.C.D/32

Actions for Hardware ACLs

The following actions are available for Hardware ACLs:

Parameter	Action
deny	Discard the packet
permit	Allow the packet
copy-to-cpu	Send a copy of the packet to the CPU and forward it as well. This is the same as copy, forward in AW hardware filters.
send-to-cpu	Send the packet to the CPU and do not forward it. This is the same as copy, discard in AlliedWare hardware filters.
send-to-mirror	Send the packet to the mirror port so packets are not switched.
copy-to-mirror	Send a copy of the packet to the mirror port and forward it as well.

Attaching Hardware ACLs to Interfaces

A hardware ACL is attached directly to a switchport using the **access-group** command. For example, to permit traffic from 192.168.1.x, but discard from 192.168.x.x:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.0/24
                any
awplus(config)# access-list 3001 deny ip 192.168.0.0/24 any
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3000
awplus(config-if)# access-group 3001
```

Hardware ACLs and QoS Classifications

Interface ACLs and QoS policies can both be attached to the same port. Where this is done, packets received on the port will be matched against the ACLs first.

The interface ACLs and QoS classifications are implemented by taking the first matching filter and applying the action defined for that filter. All subsequent matches in the table are then ignored. Thus, because ACLs are also matched first, if the matching ACL has a permit action, the packet is forwarded due to that rule's action and any subsequent QoS rules are bypassed.

You can also apply permit rules using QoS.

For example, you might want to permit a source IP address of 192.168.1.x, but block everything else on 192.168.x.x.

In this case you could create both the permit and deny rules using QoS.

Classifying Your Traffic

Classification is the process of **filtering** and **marking**. Filtering involves sorting your data into appropriate traffic types. Marking involves tagging the data so that downstream ports and routers can apply appropriate service policy rules.

There are two reasons to classify data:

1. To provide network security (Security ACLs)
2. To apply service quality criteria QoS.

Security ACLs

The main application of security ACLs is to block undesired traffic. Other applications include:

- copy-to-cpu
- copy-to-mirror
- send-to-cpu
- send-to-mirror

For more information on these applications see **"Actions for Hardware ACLs" on page 36.7**

QoS ACLs

When using ACLs though QoS, the same classification and action abilities are available, but QoS has some additional fields that it can match on (see Match Commands) and also provides the ability to perform metering, marking and remarking on packets that match the filter definitions.

The action used by a QoS class-map is determined by the ACL that is attached to it. If no ACL is attached, it uses the permit action. If an ACL is not required by the class-map (for example, only matching on the VLAN) and a deny action is required, a MAC ACL should be added with `any` for source address and `any` for destination address.

The following example creates a class-map with will deny all traffic on VLAN 2:

```
awplus(config)# access-list 4000 deny any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 4000
awplus(config-cmap)# match vlan 2
```

The default class-map matches to all traffic and so cannot have any match or ACL commands applied to it. The action for this class-map is set via the default-action command and is `permit` by default. It can be changed to `deny` by using the following commands:

```
awplus(config)# policy-map pmap1
awplus(config-pmap)# default-action deny
```

For more information on applying QoS filtering, see **"Classifying Your Data" on page 40.7**.

Attaching Hardware ACLs Using QoS

The same functionality can be achieved using QoS, by attaching the ACL to a class-map, attaching the class-map to a policy-map and attaching the policy-map to a port:

Step 1: Enable QoS on the switch

```
awplus(config)# mls qos enable
```

Step 2: Create access lists

Create ACL `3000` to permit all packets from the 192.168.1 subnet:

```
awplus(config)# access-list 3000 permit ip 192.168.1.0/24 any
```

Create ACL `3001` to deny all packets from the 192.168.0 subnet.:

```
awplus(config)# access-list 3001 deny ip 192.168.0.0/24 any
```

Step 3: Attach access-groups to class-maps

Attach ACL `3000` to the class-map `cmap1`:

```
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3000
awplus(config-cmap)# exit
```

Attach ACL `3001` to the same class-map (`cmap2`):

```
awplus(config-cmap)# match access-group 3001
awplus(config-cmap)# exit
```

Step 4: Attach class-maps to policy-maps

Attach the class-map `cmap1` to policy-map `pmap1`:

```
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# exit
```

Add the class-map `cmap2` to the policy-map `pmap1`:

```
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# exit
```

Return to Global Configuration mode:

```
awplus(config-pmap)# exit
```

Step 5: Add policy-maps to ports

Add policy-map `pmap1` to `port1.0.1`:

```
awplus(config)# interface port1.0.1
awplus(config-if)# service-policy input pmap1
```

Note that multiple interface ACLs can be attached to the same port, or either type and can be interleaved. The order of matching is based on the order in which the ACLs were attached to the port. Only one ACL can be attached to a class-map, but multiple class-maps can be attached to a policy-map. Interface ACLs can be attached to the same port as a QoS policy, with the interface ACLs being matched first as described at the beginning of the Classification section.

Filtering Hardware ACLs with QoS

Another reason for using QoS rather than interface ACLs is that QoS provides a lot more fields on which to match. These are accessed through the match commands in config-cmap mode.

Config-cmap mode describes the fields that can be matched on. Only one of each type can be matched, with the exception of tcp-flags (see below for classification). If multiple matches are specified, they are ANDed together.

The following example shows how you can match a packet on VLAN 2, that has a source IP address of 192.168.x.x and a DSCP of 12:

Create ACL `3000` to permit all packets from the 192.168 subnet.:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.0.0/16 any
```

Apply ACL 3000 to the class-map cmap1 and add the matching criteria of VLAN 2 and DSCP 12:

```
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3000
awplus(config-cmap)# match vlan 2
awplus(config-cmap)# match dscp 12
awplus(config-cmap)# exit
```

Using QoS Match Commands with TCP Flags

Usually, if multiple matches of the same type are specified, the matching process will apply to the last match that you specified. For TCP flags however, the arguments are ANDed together. For example, the following series of commands will match on a packet that has ack, syn and fin set:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match tcp-flags ack
awplus(config-cmap)# match tcp-flags syn
awplus(config-cmap)# match tcp-flags fin
awplus(config-cmap)# exit
```

The following commands will achieve the same result:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match tcp-flags ack syn fin
awplus(config-cmap)# exit
```

Note that the matching is looking to see whether "any" of the specified flags are set. There is no checking for whether any of these flags are unset. Therefore the following commands will match on a packet in any of the following combinations of syn and ack status flags as shown in the following table:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match tcp-flags syn
awplus(config-cmap)# exit
```

Syn	Ack	Match on Packet
Set	Set	Yes
Set	Unset	Yes
Unset	Set	No
Unset	Unset	No

If you want to drop packets with syn only, but not with ack and syn, the following two class-maps can be used (note that ACL 4000 is used to apply a drop action as described in **"Actions for Hardware ACLs" on page 36.7**):

Step 1: Create access lists

Create ACL `4000` to deny all packets with `any` source or destination address:

```
awplus# configure terminal
awplus(config)# access-list 4000 deny any any
```

Step 2: Create class-maps

Create the class-map `cmap1` and configure it to match on the TCP flags, `ack` and `syn`:

```
awplus(config)# class-map cmap1
awplus(config-cmap)# match tcp-flags ack syn
awplus(config-cmap)# exit
```

Create the class-map `cmap2` and configure it to match on the TCP flag, `syn`:

```
awplus(config)# class-map cmap2
awplus(config-cmap)# match tcp-flags syn
```

Step 3: Apply access-groups to class-maps

Apply ACL `4000` to this class-map (i.e. to `cmap2`):

```
awplus(config-cmap)# match access-group 4000
awplus(config-cmap)# exit
```

Step 4: Create policy-maps

Create the policy-map pmap1 and associate it with cmap1:

```
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# exit
```

Step 5: Associate class-maps with policy-maps

Associate `cmap2` with this policy-map (`pmap1`):

```
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# exit
```

ACL Filter Sequence Numbers

To help you manage ACLs you can apply sequence numbers to filters. This allows you to remove filters from named and numbered ACLs without having to reconfigure an ACL.

The ability to add sequence numbers to filters simplifies updates through the ability to position a filter within an ACL. When you add a new filter, you can specify a sequence number to position the filter in the ACL and you can also remove a current filter in an ACL by specifying a sequence number.

ACL Filter Sequence Number Behavior

- If filters with no sequence numbers are applied then the first filter is assigned a sequence number of 10, and successive filters are incremented by 10. Sequence numbers are generated automatically if they are not specified at entry.
- The maximum filter sequence number is 65535. If the sequence number exceeds this maximum, the command will not be recognized and will show the error message:
  `% Unrecognized command`
- If you enter a filter without a sequence number it is assigned a sequence number that is 10 greater than the last sequence number and is placed at the end of the ACL.
- If you enter a filter that matches an already existing filter then the first filter is overwritten with the subsequent filter.
- ACL sequence numbers determine the order of execution of filters in an ACL. Filters in a ACL with a lower value sequence number are executed before filters with a higher value.
- Output from **show running-config** displays ACL entries without filter sequence numbers. Output from relevant **show** commands displays ACL entries with their sequence numbers.
- ACL sequence numbers are re-numbered upon switch restart following a **reload** command, or after powering off and powering on the switch. ACL sequence numbers are renumbered starting from 10 and increment by 10 for each filter. See the sample output in the configuration section that follows for an illustration of this behavior. No ACL sequence number re-number command is available to perform this action.
- The ACL sequence number feature works with numbered and named standard and extended IPv4 and IPv6 access lists, plus named hardware IPv4 access lists
- The name of an access list can be designated as a number. Number in named ACLs must not exist within the range of designated numbered ACLs. (where <1-99> and <1300-1999> are standard numbered ACLs, <100-199> and <2000-2699> are extended numbered ACLs, <3000-3699> and <4000-4699> are hardware numbered ACLs).

ACL Filter Sequence Number Applicability

The ACL sequence number support feature is available with numbered and named standard and extended IPv4 and IPv6 ACLs, and the named hardware IPv4 ACLs.

Numbered standard ACLs are available in the range `<1-99>` and `<1300-1999>`, which permit or deny source addresses to control packets coming from network devices or hosts, in software.

Numbered extended ACLs are available in the range <100-199> and <2000-2699>, which permit or deny source addresses and destination addresses (plus ICMP, TCP, UDP messages) to control packets coming from and going to network devices or hosts.

Named hardware IPv4 ACLs are available which permit or deny IP and MAC source and destination addresses plus VLAN IDs to control packets coming from and going to network device and hosts. Named hardware IPv4 ACLs use the ACL sequence number support feature for ACL revision.

The ACL sequence number support feature is available for use with named hardware IPv4 ACLs, but this feature is not available for use with the numbered hardware IPv4 ACLs.

Numbered hardware ACLs are available in the range <3000-3699>, which permit or deny IP source addresses, IP destination addresses, and VLAN IDs to control packets coming from and going to network devices and hosts, in hardware.

Numbered hardware ACLs are available in the range <4000-4699>, which permit or deny MAC source addresses, MAC destination addresses, and VLAN IDs to control packets coming from and going to network devices and hosts, in hardware.

ACL Filter Sequence Number Types

There are ACL filter sequence numbers available for the following types of ACLs:

ACL Type	ACL Command Syntax
IPv4 Standard Numbered ACLs	**access-list <1-99>** **access-list <1300-1999>**
IPv4 Extended Numbered ACLs	**access-list <100-199>** **access-list <2000-2699>**
IPv4 Standard Named ACLs	**access-list standard <*name*>**
IPv4 Extended Named ACLs	**access-list extended <*name*>**
IPv4 Hardware Named ACLs	**access-list hardware <*name*>**
IPv6 Standard Named ACLs	**ipv6 access-list standard <*name*>**
IPv6 Extended Named ACLs	**ipv6 access-list extended <*name*>**

Note that ACL sequence number support for these ACL commands is optional not required. An ACL sequence number will be added automatically, starting at 10 and incrementing by 10.

ACL commands without ACL filter sequence numbers

ACL filter sequence numbers are not available for numbered hardware ACL commands:

access-list <3000-3699>

access-list <4000-4699>

ACL filter sequence number entry examples

See the below CLI entry examples for prompt sub-modes for ACL filters after ACL commands:

- To create an IPv4 Standard ACL and then define ACL filters at the IPv4 Standard ACL Configuration mode prompt **awplus(config-ip-std-acl)#**, enter the following commands:

```
awplus(config)# access-list 1
awplus(config-ip-std-acl)# permit 192.168.1.0 0.0.0.255

awplus(config)# access-list standard std_name
awplus(config-ip-std-acl)# permit 192.168.1.0/24
```

- To create an IPv4 Extended ACL and then define ACL filters at the IPv4 Extended ACL Configuration mode prompt **awplus(config-ip-ext-acl)#**, enter the following commands:

```
awplus(config)# access-list 100
awplus(config-ip-ext-acl)# permit ip 192.168.1.0 0.0.0.255
                           192.168.2.0 0.0.0.255

awplus(config)# access-list extended ext_name
awplus(config-ip-ext-acl)# permit ip 192.168.1.0 0.0.0.255
                           192.168.2.0 0.0.0.255
```

- To create an IPv4 Hardware ACL and then define ACL filters at the IPv4 Hardware ACL Configuration mode prompt **awplus(config-ip-hw-acl)#**, enter the following commands:

```
awplus(config)# access-list hardware hw_name
awplus(config-ip-hw-acl)# permit ip 192.168.1.0 0.0.0.255
                           192.168.2.0 0.0.0.255
```

- To create an IPv6 Standard ACL and then define ACL filters at the IPv6 Standard ACL Configuration mode prompt **awplus(config-ipv6-std-acl)#**, enter the following commands:

```
awplus(config)# ipv6 access-list standard ipv6_st-
                d_name
awplus(config-ipv6-std-acl)# permit 2001:db8::/64
```

- To create an IPv6 Extended ACL and then define ACL filters at the IPv6 Extended Configuration mode prompt **awplus(config-ipv6-ext-acl)#**, enter the following commands:

```
awplus(config)# ipv6 access-list extended ipv6_ex-
                t_name
awplus(config-ipv6-ext-acl)# permit ip 2001:db8::/64
                2001:db9::/64
```

ACL Filter Sequence Configuration

First create a named or numbered ACL to enter ACL filters in the ACL sub-modes available:

Step 1: Create a new ACL and add a new filter

Create ACL `10` and then add a new filter to the access-list to permit all packets from the `192.168.1` subnet:

```
                    awplus# configure terminal
             awplus(config)# access-list 10
   awplus(config-ip-std-acl)# permit 192.168.1.0 0.0.0.255
   awplus(config-ip-std-acl)# end
                    awplus# show access-list 10
```

```
Standard IP access list 10
   10 permit 192.168.1.0, wildcard bits 0.0.0.255
```

Step 2: Add another filter to the ACL

Append to, or add at the end of, ACL `10` a new filter to deny all packets from the `192.168.2` subnet:

```
                    awplus# configure terminal
             awplus(config)# access-list 10
   awplus(config-ip-std-acl)# deny 192.168.2.0 0.0.0.255
   awplus(config-ip-std-acl)# end
                    awplus# show access-list 10
```

```
Standard IP access list 10
   10 permit 192.168.1.0, wildcard bits 0.0.0.255
   20 deny   192.168.2.0, wildcard bits 0.0.0.255
```

Note that if you add a filter to an ACL without specifying a sequence number the new filter is automatically assigned a sequence number. Sequence numbers are assigned in multiples of ten from the sequence number of the last filter.

Step 3: Insert a filter into the ACL

Insert a new filter with the sequence number 15 into ACL 10 to permit packets from the 192.168.3 subnet:

```
awplus# configure terminal
awplus(config)# access-list 10
awplus(config-ip-std-acl)# 15 permit 192.168.3.0 0.0.0.255
awplus(config-ip-std-acl)# end
awplus# show access-list 10
```

```
Standard IP access list 10
   10 permit 192.168.1.0, wildcard bits 0.0.0.255
   15 permit 192.168.3.0, wildcard bits 0.0.0.255
   20 deny   192.168.2.0, wildcard bits 0.0.0.255
```

The new filter has precedence over the filter with the sequence number 20.

Step 4: Remove a filter from the ACL by specifying a filter pattern

Remove the filter with the IP address 192.168.2 from ACL 10:

```
awplus# configure terminal
awplus(config)# access-list 10
awplus(config-ip-std-acl)# no deny 192.168.2.0 0.0.0.255
awplus(config-ip-std-acl)# end
awplus# show access-list 10
```

```
Standard IP access list 10
   10 permit 192.168.1.0, wildcard bits 0.0.0.255
   15 permit 192.168.3.0, wildcard bits 0.0.0.255
```

Step 5: Remove a filter from the ACL by specifying a sequence number

Remove the filter with the sequence number 10 from ACL 10:

```
awplus# configure terminal
awplus(config)# access-list 10
awplus(config-ip-std-acl)# no 10
awplus(config-ip-std-acl)# end
awplus# show access-list
```

```
Standard IP access list 10
   15 permit 192.168.3.0, wildcard bits 0.0.0.255
```

Creating ACLs in Global Configuration Mode

You can add new filters in **Global Configuration** mode with the **access-list (standard numbered)** command on page 38.29. In this mode the filters are assigned a sequence number corresponding to the order in which they are entered, i.e. the first filter entered has higher precedence in the ACL.

Step 1: Add filters with the access-list command

Add filters to ACL `10` using the **access-list** command:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 192.168.1.0 0.0.0.255
awplus(config)# access-list 10 deny 192.168.2.0 0.0.0.255
awplus(config)# end
awplus# show access-list 10
```

```
Standard IP access list 10
   15 permit 192.168.3.0, wildcard bits 0.0.0.255
   20 permit 192.168.1.0, wildcard bits 0.0.0.255
   30 deny 192.168.2.0, wildcard bits 0.0.0.255
```

You can then enter the **IPv4 Standard ACL Configuration** mode and use the **(access-list standard numbered filter)** command on page 38.33 to specify sequence numbers to reorder the filters.

Step 2: Reorder the filters

Reorder the filters in ACL `10` by specifying a sequence number for each filter. The specified sequence number will overwrite the previous sequence number assigned to the filter:

```
awplus# configure terminal
awplus(config)# access-list 10
awplus(config-ip-std-acl)# 1021 permit 192.168.1.0 0.0.0.255
awplus(config-ip-std-acl)# 3333 permit 192.168.3.0 0.0.0.255
awplus(config-ip-std-acl)# 2772 deny 192.168.2.0 0.0.0.255
awplus(config-ip-std-acl)# end
awplus# show access-list 10
```

```
Standard IP access list 10
 1021 permit 192.168.1.0, wildcard bits 0.0.0.255
 2772 deny   192.168.2.0, wildcard bits 0.0.0.255
 3333 permit 192.168.3.0, wildcard bits 0.0.0.255
```

Step 3: Copy the running-config file into the startup-config file

Copy the running-config into the file set as the current startup-config file and then reload the device. Before the reload occurs, you will receive a confirmation request saying: "`reboot system? (y/n):`".

When the device has reboot you can then enter **Global Configuration** mode and use the **show access-list (IPv4 Software ACLs)** command to display ACL `10`:

```
awplus(config)# exit
awplus# copy running-config startup-config
awplus# reload
awplus# show access-list 10
```

```
Standard IP access list 10
   10 permit 192.168.1.0, wildcard bits 0.0.0.255
   20 deny   192.168.2.0, wildcard bits 0.0.0.255
   30 permit 192.168.3.0, wildcard bits 0.0.0.255
```

After the device has reboot the sequence numbers of the filters in the ACL have been reassigned incrementing from 10.

Display the ACL configuration details

Display the running system status and configuration details for ACLs:

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

```
!
access-list 1 deny 10.1.1.0 0.0.0.255
access-list 1 permit any
access-list 2
access-list 5
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny 192.168.2.0 0.0.0.255
access-list 10 permit 192.168.3.0 0.0.0.255
access-list 20
access-list 25 permit 10.1.2.0 0.0.0.255
access-list 25 deny 192.168.1.0 0.0.0.255
access-list 50
access-list 95 permit any
access-list 100
access-list 1300
access-list 2000
access-list extended acl
access-list extended my-list
access-list extended name
access-list extended name1
access-list standard name3
ipv6 access-list extended ipv6_acl
ipv6 access-list standard ipv6_acl2
ipv6 access-list extended my-ipv6-list
ipv6 access-list extended my-list
ipv6 access-list standard my-new-list
ipv6 access-list standard name
ipv6 access-list standard name1 deny any
ipv6 access-list extended name5
ipv6 access-list standard name6
access-list hw_acl
access-list icmp
access-list my-hw-list
access-list name2
access-list name4
!
```

For more information see **show running-config access-list** command on page 7.40.

Chapter 37: IPv4 Hardware Access Control List (ACL) Commands

Introduction 37.2
IPv4 Hardware Access List Commands and Prompts 37.3
Command List 37.4
access-group 37.4
access-list (hardware IP numbered) 37.6
access-list (hardware MAC numbered) 37.15
access-list hardware (named) 37.18
(access-list hardware ICMP filter) 37.20
(access-list hardware IP protocol filter) 37.23
(access-list hardware MAC filter) 37.29
(access-list hardware TCP UDP filter) 37.32
commit (IPv4) 37.35
show access-list (IPv4 Hardware ACLs) 37.36
show interface access-group 37.38

Introduction

This chapter provides an alphabetical reference of IPv4 Hardware Access Control List (ACL) commands. It contains detailed command information and command examples about IPv4 hardware ACLs, which are applied directly to interfaces using the **access-group** command

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself.

Notes

- Text in parenthesis in command names indicates usage not keyword entry. For example, **access-list hardware (named)** indicates named IPv4 hardware ACLs entered as `access-list hardware` <*name*> where <*name*> is a placeholder not a keyword.
- Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(access-list standard numbered filter)** represents command entry in the format shown in the syntax `[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}`.
- Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

References

For descriptions of ACLs, and further information about rules when applying them, see the **"ACL Rules" on page 36.3**.

For more information about ACL Filters, see the following references:

- **"ACL Filter Sequence Numbers" on page 36.14**
- **"ACL Filter Sequence Number Behavior" on page 36.14**
- **"Access Control Lists Introduction" on page 36.1**

For more information on link aggregation see the following references:

- **Chapter 20, Link Aggregation Introduction and Configuration**
- **Chapter 21, Link Aggregation Commands**

IPv4 Hardware Access List Commands and Prompts

Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The table **"IPv4 Hardware Access List Commands and Prompts"** shows the CLI prompts at which ACL commands are entered.

Table 37-1: IPv4 Hardware Access List Commands and Prompts

Command Name	Command Mode	Prompt
show interface access-group	Privileged Exec	`awplus#`
show access-list (IPv4 Hardware ACLs)	Privileged Exec	`awplus#`
show interface access-group	Privileged Exec	`awplus#`
access-group	Global Configuration	`awplus(config)#`
access-list (hardware IP numbered)	Global Configuration	`awplus(config)#`
access-list (hardware MAC numbered)	Global Configuration	`awplus(config)#`
access-list hardware (named)	Global Configuration	`awplus(config)#`
access-group	Interface Configuration	`awplus(config-if)#`
(access-list hardware ICMP filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware IP protocol filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware MAC filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware TCP UDP filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
commit (IPv4)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`

Command List

access-group

This command adds or removes a hardware-based access-list to or from a switch port interface. The number of hardware numbered and named access-lists that can be added to a switch port interface is determined by the available memory in hardware-based packet classification tables.

This command works in Interface Configuration mode to apply hardware access-lists to selected switch port interfaces.

The **no** variant of this command removes the selected access-list from an interface.

Syntax

```
access-group [<3000-3699>|<4000-4699>|<hardware-access-list-name>]
no access-group [<3000-3699>|4000-4699|<hardware-access-list-name>]
```

Parameter	Description
<3000-3699>	Hardware IP access-list.
<4000-4699>	Hardware MAC access-list.
<hardware-access-list-name>	The hardware access-list name.

Mode Interface Configuration for a switch port interface

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create an IP access-list that applies the appropriate permit/deny requirements with the **access-list (hardware IP numbered)** command on page 37.6, the **access-list (hardware MAC numbered)** command on page 37.15 or the **access-list hardware (named)** command on page 37.18. Then use this command to apply this hardware access-list to a specific port or port range. Note that this command will apply the access-list only to incoming data packets.

To apply ACLs to an LACP aggregated link, apply it to all the individual switch ports in the aggregated group. To apply ACLs to a static channel group, apply it to the static channel group itself. An ACL can even be applied to a static aggregated link that spans more than one switch instance (**Chapter 21, Link Aggregation Commands**).

Note that you cannot apply software standard and extended numbered ACLs to switch port interfaces with the access-group command. This command will only apply hardware ACLs.

Note Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples

To add the numbered hardware access-list `3005` to switch port interface `port1.0.1`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3005
```

To add the named hardware access-list `hw-acl` to switch port interface `port1.0.2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# access-group hw-acl
```

To apply an ACL to static channel group 2 containing switch `port1.0.5` and `port1.0.6`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-1.0.6
awplus(config-if)# static-channel-group 2
awplus(config)# interface sa2
awplus(config-if)# access-group 3000
```

Related Commands

access-list hardware (named)
access-list (hardware IP numbered)
access-list (hardware MAC numbered)
show interface access-group

access-list (hardware IP numbered)

This command creates an access-list for use with hardware classification, such as QoS. The access-list will match on either TCP or UDP type packets that have the specified source and destination IP addresses and Layer 4 port values or ranges. The parameter **any** may be specified if an address does not matter and the port values are optional.

The **no** variant of this command removes the previously specified IP hardware access-list.

Syntax [ip]

```
access-list <3000-3699> {deny|permit|copy-to-cpu|copy-to-mirror|
    send-to-mirror|send-to-cpu} ip <source> <destination>
```

Syntax [icmp]

```
access-list <3000-3699> {deny|permit|copy-to-cpu|copy-to-mirror|
    send-to-mirror|send-to-cpu} icmp <source> <destination>
    [icmp-type <type-number>]

no access-list <3000-3699>
```

Table 37-2: Parameters in the access-list (hardware IP numbered) command - ip|icmp

Parameter	Description	
<3000-3699>	Hardware IP access-list number.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
copy-to-cpu	Specify packets to copy to the CPU.	
copy-to-mirror	Specify packets to copy to the mirror port.	
send-to-mirror	Specify packets to send to the mirror port.	
send-to-cpu	Specify packets to send to the CPU.	
icmp	ICMP packet.	
ip	IP packet.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	any	Matches any source IP address.
	host *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.

Table 37-2: Parameters in the access-list (hardware IP numbered) command - ip|icmp

Parameter (cont.)	Description (cont.)	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`icmp-type`	Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.	
<type-number>	The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.

Syntax [tcp|udp]

```
access-list <3000-3699> {copy-to-cpu|copy-to-mirror|send-to-mirror|
    deny|permit|send-to-cpu} {tcp|udp} <source> {eq <sourceport>|
    lt <sourceport>|gt <sourceport>|ne <sourceport>|
    [range <start-range> <end-range>} <destination> [eq <destport>|
    lt <destport>|gt <destport>|ne <destport>]|
    [range <start-range> <end-range>]

no access-list <3000-3699>
```

Table 37-3: Parameters in the access-list (hardware IP numbered) command - tcp|udp

Parameter	Description	
<3000-3699>	Hardware IP access-list.	
copy-to-cpu	Specify packets to copy to the CPU.	
copy-to-mirror	Specify packets to copy to the mirror port.	
send-to-mirror	Specify packets to send to the mirror port.	
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.	
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.	
send-to-cpu	Specify packets to send to the CPU.	
tcp	The access-list matches only TCP packets.	
udp	The access-list matches only UDP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	any	Matches any source IP address.
	host *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.

Table 37-3: Parameters in the access-list (hardware IP numbered) command - tcp|udp

Parameter (cont.)	Description (cont.)	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source (TCP or UDP) port number, specified as an integer between 0 and 65535.	
`range`	Range of port numbers.	
<start-range>	Port number at start of range *<0-65535>*.	
<end-range>	Port number at end of range *<0-65535>*.	
<destport>	The destination (TCP or UDP) port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers that are equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers that are less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers that are greater than the port number specified immediately after this parameter.	
`ne`	Matches port numbers that are not equal to the port number specified immediately after this parameter.	

Syntax [proto]

```
access-list <3000-3699> {copy-to-cpu|copy-to-mirror|send-to-mirror|
    deny|permit|send-to-cpu}
    proto <ip-protocol> <source> <destination>

no access-list <3000-3699>
```

Table 37-4: Parameters in the access-list (hardware IP numbered) command - proto

Parameter	Description	
<3000-3699>	Hardware IP access-list.	
`copy-to-cpu`	Specify packets to copy to the CPU.	
`copy-to-mirror`	Specify packets to copy to the mirror port.	
`send-to-mirror`	Specify packets to send to the mirror port	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
`send-to-cpu`	Specify packets to send to the CPU.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 37-4: Parameters in the access-list (hardware IP numbered) command - proto

Parameter (cont.)	Description (cont.)	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`proto`	Matches only a specified type of IP Protocol <1-255>.	
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**)	
	Protocol Number	**Protocol Description [RFC Reference]**
	1	Internet Control Message [RFC792]
	2	Internet Group Management [RFC1112]
	3	Gateway-to-Gateway [RFC823]
	4	IP in IP [RFC2003]
	5	Stream [RFC1190] [RFC1819]
	6	TCP (Transmission Control Protocol) [RFC793]
	8	EGP (Exterior Gateway Protocol) [RFC888]
	9	IGP (Interior Gateway Protocol) [IANA]
	11	Network Voice Protocol [RFC741]
	17	UDP (User Datagram Protocol) [RFC768]
	20	Host monitoring [RFC869]
	27	RDP (Reliable Data Protocol) [RFC908]
	28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
	29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]

Table 37-4: Parameters in the access-list (hardware IP numbered) command - proto

Parameter (cont.)	Description (cont.)	
<ip-protocol> (cont.)	30	Bulk Data Transfer Protocol [RFC969]
	33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
	48	DSR (Dynamic Source Routing Protocol) [RFC4728]
	50	ESP (Encap Security Payload) [RFC2406]
	51	AH (Authentication Header) [RFC2402]
	54	NARP (NBMA Address Resolution Protocol) [RFC1735]
	88	EIGRP (Enhanced Interior Gateway Routing Protocol)
	89	OSPFIGP [RFC1583]
	97	Ethernet-within-IP Encapsulation / RFC3378
	98	Encapsulation Header / RFC1241
	108	IP Payload Compression Protocol / RFC2393
	112	Virtual Router Redundancy Protocol / RFC3768
	134	RSVP-E2E-IGNORE / RFC3175
	135	Mobility Header / RFC3775
	136	UDPLite / RFC3828
	137	MPLS-in-IP / RFC4023
	138	MANET Protocols / RFC-ietf-manet-iana-07.txt
	139-252	Unassigned / IANA
	253	Use for experimentation and testing / RFC3692
	254	Use for experimentation and testing / RFC3692
	255	Reserved / IANA

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage This command creates an access-list for use with hardware classification, such as when applying QoS. This command can be used to match ICMP packets, IP protocols, or TCP/UDP packets.

For ICMP packets, the <3000-3699> range IP hardware access-list will match any ICMP packet that has the specified source and destination IP addresses and ICMP type.

You may apply the **any** parameter if the source or destination IP address is not important. The ICMP type is an optional parameter.

Note Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples Follow the below example commands to configure access-lists for ICMP, IP protocol and TCP.

ICMP Example To create an access-list that will permit ICMP packets with a source address of `192.168.1.0/24` with any destination address and an ICMP type of `5` enter the below commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit icmp 192.168.1.0/24
any icmp-type 5
```

To destroy the access-list with an access-list identity of `3000` enter the below commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

IP Example To create an access-list that will permit any type of IP packet with a source address of `192.168.1.1` and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.1/32 any
```

To create an access-list that will deny all IGMP packets (IP protocol `2`) from the `192.168.0.0` network, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 deny proto 2 192.168.0.0/16
any
```

TCP Example To create an access-list that will permit TCP packets with a destination address of `192.168.1.1`, a destination port of 80 and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit tcp any 192.168.1.1/32
eq 80
```

copy-to-mirror Example

To create an access-list that will copy-to-mirror TCP packets with a destination address of `192.168.1.1`, a destination port of 80 and any source address and source port for use with the **mirror interface** command, enter the commands:

```
awplus# configure terminal

awplus(config)# access-list 3000 copy-to-mirror tcp any
192.168.1.1/32 eq 80
```

Related Commands

access-group
mirror interface
show running-config
show access-list (IPv4 Hardware ACLs)

access-list (hardware MAC numbered)

This command creates an access-list for use with hardware classification, such as QOS. The access-list will match on packets that have the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter.

The **no** variant of this command removes the specified MAC hardware filter access-list.

Syntax

```
access-list <4000-4699> {copy-to-cpu|copy-to-mirror|deny|permit|
    send-to-cpu} {<source-mac-address> <source-mac-mask>|
    any}{<destination-mac-address> <destination-mac-mask>|any}

no access-list <4000-4699>
```

Parameter	Description
<4000-4699>	Hardware MAC access-list.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`deny`	Access-list rejects packets that match the source and destination filtering.
`permit`	Access-list permits packets that match the source and destination filtering.
`send-to-cpu`	Specify packets to send to the CPU.
<source-mac-address>	The source MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each *H* is a hexadecimal number that represents a 4 bit binary number.
<source-mac-mask	The mask that will be applied to the source MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each *H* is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any source MAC address.
<destination-mac-address>	The destination MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.
<destination-mac-mask>	The mask that will be applied to the destination MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any destination MAC address.
`vlan`	Specifies that the ACL will match on the ID in the packet's VLAN tag.
<1-4094>	The VLAN VID.

Parameter (cont.)	Description (cont.)
`inner-vlan`	This parameter is used within double-tagged VLANs. It is the inner VLAN tag (VID); sometimes referred to as the C-TAG (Customer VLAN TAG), where the vlan VID tag is referred to as the S-TAG (Service VLAN TAG).
<1-4094>	The inner VLAN VID.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage This command creates an access-list for use with hardware classification, such as when applying QoS. The <4000-4699> range MAC hardware access-list will match on packets that have the specified source and destination MAC addresses. You may apply the **any** parameter if the source or destination MAC host address is not important.

Note Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples To create an access-list that will permit packets with a MAC address of `0000.00ab.1234` and any destination address enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4000 permit 0000.00ab.1234
0000.0000.0000 any
```

To create an access-list that will permit packets with an initial MAC address component of `0000.00ab` and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit 0000.00ab.1234
0000.0000.FFFF any
```

To create an access-list that will copy-to-mirror packets with an initial MAC address component of `0000.00ab` and any destination address for use with the **mirror interface** command, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 copy-to-mirror 0000.00ab.1234
0000.0000.FFFF any
```

To destroy the access-list with an access-list identity of `4000` enter the commands:

```
awplus# configure terminal
awplus(config)# no access-list 4000
```

Related Commands

access-group
mirror interface
show running-config
show access-list (IPv4 Hardware ACLs)

access-list hardware (named)

This command creates a named hardware access-list that can be applied to a switch port interface. ACL filters for a named hardware ACL are created in the IPv4 Hardware ACL Configuration mode.

The **no** variant of this command removes the specified named hardware ACL.

Syntax

```
access-list hardware <hardware-access-list-name>
no access-list hardware <hardware-access-list-name>
```

Parameter	Description
<hardware-access-list-name>	Specify the hardware ACL name to then define ACL filters for in the subsequent IPv4 Hardware ACL Configuration mode.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage Use this command to name a hardware ACL and enter the IPv4 Hardware ACL Configuration mode. If the named hardware ACL doesn't exist, it will be created after entry. If the named hardware ACL does exist, then you can enter IPv4 Hardware ACL Configuration mode for that existing ACL.

Entering this command with the hardware ACL name moves you to the `(config-ip-hw-acl)` prompt for the IPv4 Hardware ACL Configuration mode so you can enter ACL filters with sequence numbers. From this prompt, configure the filters for the ACL. See **Chapter 36, Access Control Lists Introduction** for complete examples of configured sequenced numbered ACLs.

See also the table **"IPv4 Hardware Access List Commands and Prompts" on page 37.3** in this chapter. This table shows the relevant prompts at which ACL commands and ACL filters are entered for sequenced ACLs.

Note Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples To create the hardware access-list named `ACL-1` and enter the IPv4 Hardware ACL Configuration mode to specify the ACL filter entry, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware ACL-1
awplus(config-ip-hw-acl)#
```

To remove the hardware access-list named `ACL-1`, use the commands:

```
awplus# configure terminal
awplus(config)# no access-list hardware ACL-1
```

Related Commands

access-group
(access-list hardware ICMP filter)
(access-list hardware IP protocol filter)
(access-list hardware TCP UDP filter)
(access-list standard named filter)
show access-list (IPv4 Hardware ACLs)

(access-list hardware ICMP filter)

Use this ACL filter to add a new ICMP filter entry to the current hardware access-list. The filter will match on any ICMP packet that has the specified source and destination IP addresses and ICMP type. The parameter **any** may be specified if an address does not matter and the ICMP type is an optional parameter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current hardware access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the command, the **show access-list (IPv4 Hardware ACLs)** command on page 37.36.

Syntax [icmp]

```
[<sequence-number>] {deny|permit|send-to-cpu|copy-to-cpu|
    copy-to-mirror} icmp <source> <destination> [icmp <icmp-value>]

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} icmp <source>
    <destination> [icmp <icmp-value>]

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.
`send-to-cpu`	Specify packets to send to the CPU.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`icmp`	ICMP packet type.

Parameter (cont.)	Description (cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`any`	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`any`	Matches any destination IP address.
`icmp-type`	The ICMP type.	
<icmp-value>	The value of the ICMP type.	

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage

First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the **access-group** command on page 37.4 to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note

You must reach the prompt `awplus(config-ip-hw-acl)#` by running the **access-list hardware (named)** command on page 37.18, and entering an appropriate access-list name.

Note

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples

To add an access-list filter entry with a sequence number of `100` to the access-list named `my-list` that will permit ICMP packets with a source address of `192.168.1.0/24`, any destination address and an icmp type of `5`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 100 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To remove an access-list filter entry with a sequence number of `100` in the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no 100
```

Related Commands

access-list hardware (named)
show running-config
show access-list (IPv4 Hardware ACLs)

(access-list hardware IP protocol filter)

Use this ACL filter to add an IP protocol type filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination IP addresses and IP protocol type, or has the optionally specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol type filter entry from the current hardware access-list. You can specify the IP protocol type filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP protocol type filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Hardware ACLs)** command on page 37.36.

Syntax [any|ip|proto]

```
[<sequence-number>] {deny|permit|send-to-cpu|copy-to-cpu|
   copy-to-mirror} {any|ip|proto <ip-protocol>} {<source>|
   dhcpsnooping|any} {<destination>|any} [mac {<mac-source-address>
   <mac-source-mask>|any] {<mac-destination-address>
   <mac-destination-mask>|any}

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} {any|ip|proto
   <ip-protocol>} {<source>|dhcpsnooping} {<destination>|any}
   [mac {<mac-source-address> <mac-source-mask>|any]
   {<mac-destination-address> <mac-destination-mask>|any}

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Access-list rejects packets of the type specified.
permit	Access-list allows packets of the type specified
send to cpu	Specify packets to send to the CPU.
copy to cpu	Specify packets to copy to the CPU.
copy to mirror	Specify packets to copy to the mirror port.
ip	IP packets.
any	Any packet.
proto *<ip-protocol>*	The IP Protocol type specified by it protocol number <1-255>.

Parameter (cont.)	Description (cont.)	
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**)	
	Protocol Number	**Protocol Description [RFC Reference]**
	1	Internet Control Message [RFC792]
	2	Internet Group Management [RFC1112]
	3	Gateway-to-Gateway [RFC823]
	4	IP in IP [RFC2003]
	5	Stream [RFC1190] [RFC1819]
	6	TCP (Transmission Control Protocol) [RFC793]
	8	EGP (Exterior Gateway Protocol) [RFC888]
	9	IGP (Interior Gateway Protocol) [IANA]
	11	Network Voice Protocol [RFC741]
	17	UDP (User Datagram Protocol) [RFC768]
	20	Host monitoring [RFC869]
	27	RDP (Reliable Data Protocol) [RFC908]
	28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
	29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
	30	Bulk Data Transfer Protocol [RFC969]
	33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
	48	DSR (Dynamic Source Routing Protocol) [RFC4728]
	50	ESP (Encap Security Payload) [RFC2406]
	51	AH (Authentication Header) [RFC2402]

Parameter (cont.)	Description (cont.)	
<ip-protocol> (cont.)	54	NARP (NBMA Address Resolution Protocol) [RFC1735]
	58	ICMP for IPv6 [RFC1883]
	59	No Next Header for IPv6 [RFC1883]
	60	Destination Options for IPv6 [RFC1883]
	88	EIGRP (Enhanced Interior Gateway Routing Protocol)
	89	OSPFIGP [RFC1583]
	97	Ethernet-within-IP Encapsulation / RFC3378
	98	Encapsulation Header / RFC1241
	108	IP Payload Compression Protocol / RFC2393
	112	Virtual Router Redundancy Protocol / RFC3768
	134	RSVP-E2E-IGNORE / RFC3175
	135	Mobility Header / RFC3775
	136	UDPLite / RFC3828
	137	MPLS-in-IP / RFC4023
	138	MANET Protocols / RFC-ietf-manet-iana-07.txt
	139-252	Unassigned / IANA
	253	Use for experimentation and testing / RFC3692
	254	Use for experimentation and testing / RFC3692
	255	Reserved / IANA
`dhcpsnooping`	The source address learned from the DHCP Snooping binding database.	

Parameter (cont.)	Description (cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`mac`	Signifies a MAC and based hardware access-list.	
<mac-source-address>	The source host's MAC address, entered in HHHH.HHHH.HHHH format.	
<mac-source-mask>	The source host's MAC wildcard mask entered in HHHH.HHHH.HHHH format. where Hex `FF` = Ignore, and Hex `00` = Match.	

Parameter (cont.)	Description (cont.)
`any`	Matches any source MAC address.
`<mac-destination-address>`	The destination host's MAC address, entered in HHHH.HHHH.HHHH format.
`<mac-destination-mask>`	The destination host's wildcard mask entered in HHHH.HHHH.HHHH format. where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Matches any destination MAC address.

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the **access-group** command on page 37.4 to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note
The access control list being configured is selected by running the **access-list hardware (named)** command on page 37.18. with the required access control list number, or name, but with no further parameters selected.

Note
Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of `192.168.1.1` and any destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any
```

To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of `192.168.1.1` and a MAC source address of `ffee.ddcc.bbaa` with any IP and MAC destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any mac
ffee.ddcc.bbaa any
```

To add an access-list filter entry to the access-list named `my-list` a filter that will deny all IGMP packets (protocol `2`) from the `192.168.0.0` network with sequence number `50` in access-list, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 50 deny proto 2 192.168.0.0/16 any
```

Related Commands

access-list hardware (named)
show running-config
show access-list (IPv4 Hardware ACLs)

(access-list hardware MAC filter)

Use this ACL filter to add a MAC filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a MAC filter entry from the current hardware access-list. You can specify the MAC filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its MAC filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Hardware ACLs)** command on page 37.36.

Syntax [mac]

```
[<sequence-number>] {deny|permit|send-to-cpu|copy-to-cpu|
    copy-to-mirror} mac {<source-mac-address> <source-mac-mask>|any}
    {<destination-mac-address> <destination-mac-mask>|any}

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
    mac {<source-mac-address> <source-mac-mask>|any}
    {<destination-mac-address> <destination-mac-mask>|any}

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specify packets to reject.
permit	Specify packets to accept.
send-to-cpu	
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the CPU.
mac	MAC address.
<source-mac-address>	The source MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.
<source-mac-mask>	The mask that will be applied to the source MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
any	Any source MAC host.
<destination-mac-address>	The destination MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.

Parameter(cont.)	Description(cont.)
<destination-mac-mask>	The mask that will be applied to the destination MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any destination MAC host.

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the **access-group** command on page 37.4 to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number

Note
The access control list being configured is selected by running the **access-list hardware (named)** command on page 37.18. with the required access control list number, or name, but with no further parameters selected.

Note
Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples To add an access-list filter entry to the access-list named `my-list` that will permit packets with a source MAC address of `0000.00ab.1234` and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit mac 0000.00ab.1234
0000.0000.0000 any
```

To remove an access-list filter entry that permit packets with a source MAC address of `0000.00ab.1234` and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no permit mac 0000.00ab.1234
0000.0000.0000 any
```

Related Commands

access-group
access-list hardware (named)
show running-config

(access-list hardware TCP UDP filter)

Use this ACL filter to add a TCP or UDP filter entry to the current hardware access-list. The filter will match on any TCP or UDP type packet that has the specified source and destination IP addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current hardware access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Hardware ACLs)** command on page 37.36.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit|send-to-cpu|copy-to-cpu|
   copy-to-mirror} {tcp|udp} [<source>|eq <sourceport>|
   gt <sourceport>|lt <sourceport>|ne <sourceport>|
   range <start-range> <end-range>] [<destination>|eq <destport>|
   gt <destport>|lt <destport>|ne <destport>|
   range <start-range> <end-range>]

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} {tcp|udp}
   [<source>|eq <sourceport>|gt <sourceport>|lt <sourceport>|
   ne <sourceport>|range <start-range> <end-range>] [<destination>|
   eq <destport>|gt <destport>|lt <destport>|ne <destport>|
   range <start-range> <end-range>]

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Access-list rejects packets that match the source and destination filtering specified with this command.
permit	Access-list permits packets that match the source and destination filtering specified with this command.
send-to-cpu	Specify packets to send to the CPU.
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the mirror port.
tcp	TCP packets.
udp	UDP packets.

Parameter(cont.)	Description(cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source TCP or UDP port number, specified as an integer between 0 and 65535.	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`eq`	Equal to.	
`lt`	Less than.	
`gt`	Greater than.	

Parameter(cont.)	Description(cont.)
`ne`	Not equal to.
<destport>	The source TCP or UDP port number, specified as an integer between 0 and 65535.
`range`	Specify the range of port numbers between 0 and 65535.
<start-range>	The source or destination port number at the start of the range *<0-65535>*.
<end-range>	The source or destination port number at the end of the range *<0-65535>*.

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the **access-group** command on page 37.4 to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note
The access control list being configured is selected by running the **access-list hardware (named)** command on page 37.18. with the required access control list number, or name, but with no further parameters selected.

Note
Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Example To add an access-list filter entry to access-list named `my-hw-list` that will permit TCP packets with a destination address of `192.168.1.1`, a destination port of `80`, and any source address, and source port, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# permit tcp any 192.168.1.1/32 eq 80
```

Related Commands
access-list hardware (named)
show running-config
show access-list (IPv4 Hardware ACLs)

commit (IPv4)

Use this command to commit the IPv4 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv4 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv4 ACLs to synchronize.

Syntax `commit`

Mode IPv4 Hardware ACL Configuration

Usage Normally, when an IPv4 hardware ACL is edited, the new configuration state of the IPv4 ACL is not written to hardware until you exit IPv4 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the **exit** command to exit configuration modes, potentially leading to IPv4 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv4 hardware ACL filter ensures that it is updated in the hardware immediately.

Example To update the hardware with the IPv4 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# commit
```

Related Commands **access-list hardware (named)**

show access-list (IPv4 Hardware ACLs)

Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

Syntax

```
show access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|
    <3000-3699>|<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related Commands

access-list extended (named)
access-list (hardware MAC numbered)
access-list hardware (named)

show interface access-group

Use this command to display the access groups attached to a port. If an access group is specified, then the output only includes the ports that the specified access group is attached to. If no access group is specified then this command displays all access groups that are attached to the ports that are specified with *<port-list>*.

Note that **access group** is the term given for an access-list when it is applied to an interface.

Note This command will function on your switch in stand-alone mode. but is not supported when the device forms part of a VCStack.

Syntax

```
show interface <port-list> access-group [<3000-3699>|<4000-4699>]
```

Parameter	Description
<port-list>	Specify the ports to display information. A port-list can be either: ■ a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2) ■ a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6 or port1.0.1-port1.0.6 or po1-po2 ■ a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.3-1.0.6. Do not mix switch ports, static channel groups, and LACP channel groups in the same list.
`access group`	Select the access group whose details you want to show.
<3000-3699>	Specifies the Hardware IP access-list.
<4000-4699>	Specifies the Hardware MAC access-list.

Mode User Exec and Privileged Exec

Example To show all access-lists attached to `port1.0.1`, use the command:

```
awplus# show interface port1.0.1 access-group
```

Output **Figure 37-1: Example output from the show interface access-group command**

```
Interface port1.0.1
  access-group 3000
  access-group 3002
  access-group 3001
```

Related Commands access-group

Chapter 38: IPv4 Software Access Control List (ACL) Commands

Introduction 38.2
IPv4 Software Access List Commands and Prompts 38.3
Command List 38.4
access-list extended (named) 38.4
access-list (extended numbered) 38.12
(access-list extended ICMP filter) 38.15
(access-list extended IP filter) 38.17
(access-list extended IP protocol filter) 38.20
(access-list extended TCP UDP filter) 38.24
access-list standard (named) 38.27
access-list (standard numbered) 38.29
(access-list standard named filter) 38.31
(access-list standard numbered filter) 38.33
clear ip prefix-list 38.35
maximum-access-list 38.36
show access-list (IPv4 Software ACLs) 38.37
show ip access-list 38.39

Introduction

This chapter provides an alphabetical reference for the IPv4 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv4 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

Note

See **Chapter 36, Access Control Lists Introduction** for descriptions of ACLs, and for further information about rules when applying ACLs see the **ACL Rules** section.

See **ACL Filter Sequence Numbers** and **ACL Filter Sequence Number Behavior** sections in **Chapter 36, Access Control Lists Introduction** about ACL Filters.

See all relevant Routing commands and configurations in **"IPv4 Software Access Control List (ACL) Commands"** and all relevant Multicast commands and configurations in **"Multicast Applications"**.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see **Chapter 20, Link Aggregation Introduction and Configuration**, and **Chapter 21, Link Aggregation Commands**.

Note

Text in parenthesis in command names indicates usage not keyword entry. For example, **access-list hardware (named)** indicates named IPv4 hardware ACLs entered as `access-list hardware` <*name*> where <*name*> is a placeholder not a keyword.

Note

Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(access-list standard numbered filter)** represents command entry in the format shown in the syntax `[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}`.

Note

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

IPv4 Software Access List Commands and Prompts

Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 38-1: IPv4 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ip access-list	Privileged Exec	`awplus#`
access-group	Global Configuration	`awplus(config)#`
access-list (extended numbered)	Global Configuration	`awplus(config)#`
access-list standard (named)	Global Configuration	`awplus(config)#`
access-list (standard numbered)	Global Configuration	`awplus(config)#`
maximum-access-list	Global Configuration	`awplus(config)#`
(access-list extended ICMP filter)	IPv4 Extended ACL Configuration	`awplus(config-ip-ext-acl)#`
(access-list extended IP filter)	IPv4 Extended ACL Configuration	`awplus(config-ip-ext-acl)#`
(access-list extended IP protocol filter)	IPv4 Extended ACL Configuration	`awplus(config-ip-ext-acl)#`
(access-list extended TCP UDP filter)	IPv4 Extended ACL Configuration	`awplus(config-ip-ext-acl)#`
(access-list standard named filter)	IPv4 Standard ACL Configuration	`awplus(config-ip-std-acl)#`
(access-list standard numbered filter)	IPv4 Standard ACL Configuration	`awplus(config-ip-std-acl)#`

Command List

access-list extended (named)

This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list name.

The **no** variant of this command removes a specified extended named access-list.

Syntax [list-name]

```
access-list extended <list-name>

no access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the access-list

Syntax [icmp]

```
access-list extended <list-name>{deny|permit}
   icmp <source> <destination> [icmp-type <type-number>] [log]

no access-list extended <list-name>{deny|permit}
   icmp <source> <destination> [icmp-type <type-number>] [log]
```

Table 38-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description
<list-name>	A user-defined name for the access-list.
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.
icmp	The access-list matches only ICMP packets.
icmp-type	Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.

Table 38-2: Parameters in the access-list extended (named) command - icmp (cont.)

Parameter(cont.)	Description(cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 38-2: Parameters in the access-list extended (named) command - icmp (cont.)

Parameter(cont.)	Description(cont.)	
<type-number>	The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
log	Logs the results.	

Syntax [tcp|udp]

```
access-list extended <list-name> {deny|permit} {tcp|udp} <source>
   [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne <sourceport>]
   <destination> [eq <destport>|lt <destport>|gt <destport>|
   ne <destport>] [log]

no access-list extended <list-name> {deny|permit} {tcp|udp} <source>
   [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne <sourceport>]
   <destination> [eq <destport> |lt <destport>|gt <destport>|ne
   <destport>][log]
```

Table 38-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description
<list-name>	A user-defined name for the access-list.
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.
tcp	The access-list matches only TCP packets.
udp	The access-list matches only UDP packets.

Table 38-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter(cont.)	Description(cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/` *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/` *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	

Table 38-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter(cont.)	Description(cont.)
`ne`	Matches port numbers not equal to the port number specified immediately after this parameter.
`log`	Log the results.

Syntax [proto|any|ip]

```
access-list extended <list-name> {deny|permit} {proto <ip-protocol>|
   any|ip} {<source>} {<destination>} [log]

no access-list extended <list-name>{deny|permit}
   {proto <ip-protocol>|any|ip}{<source>}{<destination>}[log]
```

Table 38-4: Parameters in the access-list extended (named) command - proto|ip|any

Parameter	Description	
<list-name>	A user-defined name for the access-list.	
`deny`	The access-list rejects packets that match the type, source, and destination filtering specified with this command.	
`permit`	The access-list permits packets that match the type, source, and destination filtering specified with this command.	
`proto`	Matches only a specified type of IP Protocol.	
`any`	The access-list matches any type of IP packet.	
`ip`	The access-list matches only IP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/ <prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 38-4: Parameters in the access-list extended (named) command - proto|ip|any

Parameter (cont.)	Description (cont.)	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`log`	Logs the results.	
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**)	
	Protocol Number	**Protocol Description [RFC Reference]**
	`1`	Internet Control Message [RFC792]
	`2`	Internet Group Management [RFC1112]
	`3`	Gateway-to-Gateway [RFC823]
	`4`	IP in IP [RFC2003]
	`5`	Stream [RFC1190] [RFC1819]
	`6`	TCP (Transmission Control Protocol) [RFC793]
	`8`	EGP (Exterior Gateway Protocol) [RFC888]
	`9`	IGP (Interior Gateway Protocol) [IANA]
	`11`	Network Voice Protocol [RFC741]
	`17`	UDP (User Datagram Protocol) [RFC768]
	`20`	Host monitoring [RFC869]
	`27`	RDP (Reliable Data Protocol) [RFC908]
	`28`	IRTP (Internet Reliable Transaction Protocol) [RFC938]
	`29`	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
	`30`	Bulk Data Transfer Protocol [RFC969]

Table 38-4: Parameters in the access-list extended (named) command - proto|ip|any

Parameter (cont.)	Description (cont.)	
<ip-protocol> (cont.)	**Protocol Number**	**Protocol Description [RFC Reference]**
	33	Datagram Congestion Control Protocol [RFC4340]
	48	DSR (Dynamic Source Routing Protocol) [RFC4728]
	50	ESP (Encap Security Payload) [RFC2406]
	51	AH (Authentication Header) [RFC2402]
	54	NARP (NBMA Address Resolution Protocol) [RFC1735]
	88	EIGRP (Enhanced Interior Gateway Routing Protocol)
	89	OSPFIGP [RFC1583]
	97	Ethernet-within-IP Encapsulation / RFC3378
	98	Encapsulation Header / RFC1241
	108	IP Payload Compression Protocol / RFC2393
	112	Virtual Router Redundancy Protocol / RFC3768
	134	RSVP-E2E-IGNORE / RFC3175
	135	Mobility Header / RFC3775
	136	UDPLite / RFC3828
	137	MPLS-in-IP / RFC4023
	138	MANET Protocols / RFC-ietf-manet-iana-07.txt
	139-252	Unassigned / IANA
	253	Use for experimentation and testing / RFC3692
	254	Use for experimentation and testing / RFC3692
	255	Reserved / IANA

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter **access-list** followed by only the number. This latter method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands **(access-list extended ICMP filter)**, **(access-list extended IP filter)**, and **(access-list extended IP protocol filter)**.

The table **"IPv4 Software Access List Commands and Prompts" on page 38.3** shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note that packets must match both the source and the destination details.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK deny tcp 2.2.2.3/24 eq
14 3.3.3.4/24 eq 12 log
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK
awplus(config-ip-ext-acl)# deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24
eq 12 log
```

Related Commands
(access-list extended ICMP filter)
(access-list extended IP filter)
(access-list extended TCP UDP filter)
show running-config
show ip access-list

access-list (extended numbered)

This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list number.

The **no** variant of this command removes a specified extended named access-list.

Syntax [list-number]

```
access-list {<100-199>|<2000-2699>}

no access-list {<100-199>|<2000-2699>}
```

Parameter	Description
<100-199>	IP extended access-list.
<2000-2699>	IP extended access-list (expanded range).

Syntax [deny|permit]

```
access-list {<100-199>|<2000-2699>} {deny|permit} ip <source>
   <destination>

no access-list {<100-199>|<2000-2699>}{deny|permit} ip <source>
   <destination>
```

Parameter	Description	
<100-199>	IP extended access-list.	
<2000-2699>	IP extended access-list (expanded range).	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any source IP address within the specified subnet.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	

Parameter (cont.)	Description (cont.)	
	`any`	Matches any destination IP address.
	`host <ip-addr>`	Matches a single destination host with the IP address given by `<ip-addr>` in dotted decimal notation.
	`<ip-addr> <reverse-mask>`	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any destination IP address within the specified subnet.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter **access-list** followed by only the number. This latter method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands **(access-list extended ICMP filter)**, **(access-list extended IP filter)**, and **(access-list extended IP protocol filter)**.

The table **"IPv4 Software Access List Commands and Prompts" on page 38.3** shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note that packets must match both the source and the destination details.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as in previous software releases as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101 deny ip 172.16.10.0 0.0.0.255
any
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# deny ip 172.16.10.0 0.0.0.255 any
```

Related Commands

(access-list extended ICMP filter)
(access-list extended IP filter)
(access-list extended TCP UDP filter)
show running-config
show ip access-list

(access-list extended ICMP filter)

Use this ACL filter to add a new ICMP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current extended access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax [icmp]

```
[<sequence-number>] {deny|permit} icmp <source> <destination>
    [icmp-type <icmp-value>] [log]

no {deny|permit} icmp <source> <destination>[icmp-type <icmp-value>]
    [log]

no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
icmp	ICMP packet type.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	any	Matches any destination IP address.
icmp-type	The ICMP type.	

Parameter (cont.)	Description (cont.)
<icmp-value>	The value of the ICMP type.
log	Log the results.

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note The access control list being configured is selected by running the **access-list (extended numbered)** command or the **access-list extended (named)** command, with the required access control list number, or name - but with no further parameters selected.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To add a new entry in access-list called `my-list` that will reject ICMP packets from `10.0.0.1` to `192.168.1.1`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny icmp 10.0.0.1/32 192.168.1.1/32
```

Use the following commands to add a new filter at sequence number `5` position of the access-list called `my-list`. The filter will accept the ICMP type `8` packets from `10.1.1.0/24` network, to `192.168.1.0` network:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit icmp 10.1.1.0/24
                           192.168.1.0/24 icmp-type 8
```

Related Commands **access-group**
show running-config
show ip access-list

(access-list extended IP filter)

Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax [ip]

```
[<sequence-number>] {deny|permit} ip <source> <destination>
no {deny|permit} ip <source> <destination>
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.

Mode Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note

The access control list being configured is selected by running the **access-list (extended numbered)** command or the **access-list extended (named)** command, with the required access control list number, or name - but with no further parameters selected.

Note

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example 1 [list-number] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a numbered extended access-list `101`:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the numbered extended access-list `101` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
                           192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 2 [list-name] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a named access-list called `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the named access-list `my-acl` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
                           192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 3 [list-number] Use the following commands to remove the access-list filter entry with sequence number `20` from extended numbered access-list `101`.

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# no 20
```

Example 4 [list-name] Use the following commands to remove the access-list filter entry with sequence number `20` from extended named access-list `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)# no 20
```

Related Commands

access-list extended (named)
access-list (extended numbered)
show running-config
show ip access-list

(access-list extended IP protocol filter)

Use this ACL filter to add a new IP protocol type filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax [proto]

```
[<sequence-number>] {deny|permit} proto <ip-protocol> <source>
   <destination> [log]

no {deny|permit} proto <ip-protocol> <source> <destination> [log]

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.
`proto` *<ip-protocol>*	The IP Protocol type specified by its protocol number <1-255>.
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**).

Protocol Number	Protocol Description [RFC Reference]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]

Parameter (cont.)	Description (cont.)	
<ip-protocol> (cont.)	17	UDP (User Datagram Protocol) [RFC768]
	20	Host monitoring [RFC869]
	27	RDP (Reliable Data Protocol) [RFC908]
	28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
	29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
	30	Bulk Data Transfer Protocol [RFC969]
	33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
	48	DSR (Dynamic Source Routing Protocol) [RFC4728]
	50	ESP (Encap Security Payload) [RFC2406]
	51	AH (Authentication Header) [RFC2402]
	54	NARP (NBMA Address Resolution Protocol) [RFC1735]
	88	EIGRP (Enhanced Interior Gateway Routing Protocol)
	89	OSPFIGP [RFC1583]
	97	Ethernet-within-IP Encapsulation / RFC3378
	98	Encapsulation Header / RFC1241
	108	IP Payload Compression Protocol / RFC2393
	112	Virtual Router Redundancy Protocol / RFC3768
	134	RSVP-E2E-IGNORE / RFC3175
	135	Mobility Header / RFC3775
	136	UDPLite / RFC3828
	137	MPLS-in-IP / RFC4023
	138	MANET Protocols / RFC-ietf-manet-iana-07.txt
	139-252	Unassigned / IANA
	253	Use for experimentation and testing / RFC3692
	254	Use for experimentation and testing / RFC3692
	255	Reserved / IANA

Parameter (cont.)	Description (cont.)	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	any	Matches any destination IP address.
log	Log the results.	

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note The access control list being configured is selected by running the **access-list (extended numbered)** command or the **access-list extended (named)** command, with the required access control list number, or name - but with no further parameters selected.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example 1 [creating a list] Use the following commands to add a new access-list filter entry to the access-list named `my-list` that will reject IP packets from source address `10.10.1.1/32` to destination address `192.68.1.1/32`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny ip 10.10.1.1/32 192.168.1.1/32
```

Example 2 [adding to a list]

Use the following commands to add a new access-list filter entry at sequence position `5` in the access-list named `my-list` that will accept packets from source address `10.10.1.1/24` to destination address `192.68.1.1/24`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit ip 10.10.1.1/24 192.168.1.1/
24
```

Related Commands

access-list extended (named)
access-list (extended numbered)
show running-config
show ip access-list

(access-list extended TCP UDP filter)

Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current extended access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp} <source> {eq <sourceport>
    |lt <sourceport>|gt <sourceport>|ne <sourceport>} <destination>
    [eq <destport>|lt <destport>|gt <destport>|ne <destport>] [log]

no [<sequence-number>]{deny|permit} {tcp|udp} <source> {eq
    <sourceport> |lt <sourceport>|gt <sourceport>|ne
    <sourceport>}<destination> [eq <destport>|lt <destport>|gt
    <destport>|ne <destport>] [log]

no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
tcp	The access-list matches only TCP packets.	
udp	The access-list matches only UDP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	

Parameter (cont.)	Description (cont.)	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	`any`	Matches any destination IP address.
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	
`ne`	Matches port numbers not equal to the port number specified immediately after this parameter.	
`log`	Log the results.	

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note The access control list being configured is selected by running the **access-list (extended numbered)** command or the **access-list extended (named)** command, with the required access control list number, or name - but with no further parameters selected.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example 1 [creating a list] To add a new entry to the access-list named `my-list` that will reject TCP packets from `10.0.0.1` on TCP port `10` to `192.168.1.1` on TCP port `20`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny tcp 10.0.0.1/32 eq 10
                           192.168.1.1/32 eq 20
```

Example 2 [adding to a list]

To insert a new entry with sequence number `5` of the access-list named `my-list` that will accept UDP packets from `10.1.1.0/24` network to `192.168.1.0/24` network on UDP port `80`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit udp 10.1.1.0/24
192.168.1.0/24 eq 80
```

Related Commands

access-list extended (named)
access-list (extended numbered)
show running-config
show ip access-list

access-list standard (named)

This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can either create a standard named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list name.

The **no** variant of this command removes a specified standard named access-list.

Syntax [list-name]

```
access-list standard <standard-access-list-name>

no access-list standard <standard-access-list-name>
```

Parameter	Description
<standard-access-list-name>	Specify a name for the standard access-list.

Syntax [deny|permit]

```
access-list standard <standard-access-list-name> {deny|permit}
    <source>

no access-list standard <standard-access-list-name> {deny|permit}
    <source>
```

Parameter	Description	
<standard-access-list-name>	Specify a name for the standard access-list.	
deny	The access-list rejects packets that match the source filtering specified with this command.	
permit	The access-list permits packets that match the source filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring a standard named access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by only the standard access-list name then enter. This latter method moves you to the IPv4 Standard ACL Configuration mode for the selected standard named access-list, and from here you can configure the deny or permit filters for this selected standard named access-list.

See the table **"IPv4 Software Access List Commands and Prompts" on page 38.3** in this chapter which shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To define a standard access-list named `my-list` and deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list deny any
```

Alternatively, to define a standard access-list named `my-list` and enter the IPv4 Standard ACL Configuration mode to deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 5 deny any
```

Related Commands
(access-list standard named filter)
show running-config
show ip access-list

access-list (standard numbered)

This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can either create a standard numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list number.

The **no** variant of this command removes a specified standard numbered access-list.

Syntax [list-number]

```
access-list {<1-99>|<1300-1999>}
no access-list {<1-99>|<1300-1999>}
```

Parameter	Description
<1-99>	IP standard access-list.
<1300-1999>	IP standard access-list (expanded range).

Syntax [deny|permit]

```
access-list {<1-99>|<1300-1999>} {deny|permit} <source>
no access-list {<1-99>|<1300-1999>} {deny|permit} <source>
```

Parameter	Description	
<1-99>	IP standard access-list.	
<1300-1999>	IP standard access-list (expanded range).	
`deny`	Access-list rejects packets from the specified source.	
`permit`	Access-list accepts packets from the specified source.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	Enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`any`	Matches any source IP address.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring a standard numbered access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by only the standard access-list name. This moves you to the IPv4 Standard ACL Configuration mode for the selected standard numbered access-list, and from here you can configure the deny or permit filters for this selected standard numbered access-list.

See the table **"IPv4 Software Access List Commands and Prompts" on page 38.3** in this chapter which shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To create ACL number `67` that will deny packets from subnet `172.16.10`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67 deny 172.16.10.0 0.0.0.255
```

Alternatively, to enter the IPv4 Standard ACL Configuration mode to create the ACL filter and deny packets from subnet `172.16.10.0` for the standard numbered access-list `67`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67
awplus(config-ip-std-acl)# deny 172.16.10.0 0.0.0.255
```

Related Commands
(access-list standard named filter)
show running-config
show ip access-list

(access-list standard named filter)

This ACL filter adds a source IP address filter entry to a current named standard access-list. If the sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current named standard access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax

```
[<sequence-number>] {deny|permit} {<source> [exact-match]|any}
no {deny|permit} {<source> [exact-match]|any}
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets of the source filtering specified.	
permit	Access-list allows packets of the source filtering specified	
<source>	The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr>	An IPv4 address in a.b.c.d format.
exact-match	Specify an exact IP prefix to match on.	
any	Matches any source IP address.	

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note

The access control list being configured is selected by running the **access-list standard (named)** command with the required access control list number, or name, but with no further parameters selected.

Note

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples Use the following commands to add a new filter entry to access-list `my-list` that will reject IP address `10.1.1.1`:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# deny 10.1.1.1/32
```

Use the following commands to insert a new filter entry into access-list `my-list` at sequence position number `15` that will accept IP network `10.1.2.0`:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 15 permit 10.1.2.0/24
```

Related Commands

access-list standard (named)
show running-config
show ip access-list

(access-list standard numbered filter)

This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current standard numbered access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

Syntax

```
[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}
no {deny|permit} {<source>|host <host-address>|any}
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets of the type specified.	
permit	Access-list allows packets of the type specified	
<source>	The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	Enter a reverse mask for the source address in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	<ip-addr>	An IPv4 address in a.b.c.d format.
host	A single source host.	
<host-address>	Single source host address.	
any	Matches any source IP address.	

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

Note The access control list being configured is selected by running the **access-list standard (named)** command with the required access control list number, or name, but with no further parameters selected.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example To add a new entry accepting the IP network `10.1.1.0/24` at the sequence number `15` position, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 99
awplus(config-ip-std-acl)# 15 permit 10.1.2.0 0.0.0.255
```

Related Commands
access-list (standard numbered)
show running-config
show ip access-list

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries.

Syntax `clear ip prefix-list [<list-name>] [<ip-address>/<mask>]`

Parameter	Description
<list-name>	The name of the prefix-list.
<ip-address>/<mask>	The IP prefix and length.

Mode Privileged Exec

Example To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```

maximum-access-list

Sets the maximum number of filters that can be added to any access-list. These are access-lists within the ranges <1-199>, <1300-1999> and <2000-2699> and named standard and extended access-lists.

The **no** variant of this command removes the limit on the number of filters that can be added to a software access-list

Syntax

```
maximum-access-list <1-4294967294>
no maximum-access-list
```

Parameter	Description
<1-4294967294>	Filter range.

Mode Global Configuration

Example To set the maximum number of software filters to `200`:

```
awplus# configure terminal
awplus(config)# maximum-access-list 200
```

show access-list (IPv4 Software ACLs)

Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list

Syntax

```
show access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|
    <3000-3699>|<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related Commands

access-list standard (named)
access-list (standard numbered)
access-list (extended numbered)

show ip access-list

Use this command to display IP access-lists.

Syntax

```
show ip access-list [<1-99>|<100-199>|<1300-1999>|<2000-2699>|
    <access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (expanded range).
<2000-2699>	IP extended access-list (expanded range).
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip access-list
```

Output **Figure 38-1: Example output from the show ip access-list command**

```
Standard IP access-list 1
    permit 172.168.6.0, wildcard bits 0.0.0.255
    permit 192.168.6.0, wildcard bits 0.0.0.255
```

Chapter 39: IPv6 Software Access Control List (ACL) Commands

Introduction 39.2
IPv6 Software Access List Commands and Prompts 39.3
Command List 39.4
ipv6 access-list extended (named) 39.4
ipv6 access-list extended proto 39.8
(ipv6 access-list extended IP protocol filter) 39.11
(ipv6 access-list extended TCP UDP filter) 39.14
ipv6 access-list standard (named) 39.16
(ipv6 access-list standard filter) 39.18
show ipv6 access-list (IPv6 Software ACLs) 39.20

Introduction

This chapter provides an alphabetical reference for the IPv6 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

Note

See **Chapter 36, Access Control Lists Introduction** for descriptions of ACLs, and for further information about rules when applying ACLs see the **ACL Rules** section.

See **ACL Filter Sequence Numbers** and **ACL Filter Sequence Number Behavior** sections in **Chapter 36, Access Control Lists Introduction** about ACL Filters.

See all relevant Routing commands and configurations in **"IP and IPv6"** and all relevant Multicast commands and configurations in **"Multicast Applications"**.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see **Chapter 20, Link Aggregation Introduction and Configuration**, and **Chapter 21, Link Aggregation Commands**.

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where `<name>` is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI. For example, **(ipv6 access-list standard IPv6 filter)** represents command entry in the format:

`[<sequence-number>] {deny|permit} {<IPv6-source-address/prefix-length>|any}.`

Note

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

IPv6 Software Access List Commands and Prompts

Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The table **"IPv6 Software Access List Commands and Prompts"** shows the CLI prompts at which ACL commands are entered.

Table 39-1: IPv6 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ipv6 access-list (IPv6 Software ACLs)	Privileged Exec	`awplus#`
ipv6 access-list extended (named)	Global Configuration	`awplus(config)#`
ipv6 access-list standard (named)	Global Configuration	`awplus(config)#`
(ipv6 access-list extended IP protocol filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list extended TCP UDP filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list standard filter)	IPv6 Standard ACL Configuration	`awplus(config-ipv6-std-acl)#`

Command List

ipv6 access-list extended (named)

Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny IP, ICMP, TCP, UDP packets or ICMP packets with a specific value based on the source or destination.

The **no** variant of this command removes a specified IPv6 extended access-list.

Syntax [list-name]

```
ipv6 access-list extended <list-name>

no ipv6 access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.

Syntax [any|icmp|ip]

```
ipv6 access-list extended <list-name> {deny|permit} {any|icmp|ip}
   {<ipv6-source-address/prefix-length>|any}
   {<ipv6-destination-address/prefix-length>|any}
   [<icmp-type <icmp-type>][log]

no ipv6 access-list extended <list-name> {deny|permit} {any|icmp|ip}
   {<ipv6-source-address/prefix-length>|any}
   {<ipv6-destination-address/prefix-length>|any}
   [<icmp-type <icmp-type>][log]
```

Syntax [tcp|udp]

```
ipv6 access-list extended <list-name> {deny|permit} {tcp|udp}
   {<ipv6-source-address/prefix-length>|any} {eq <sourceport>|
   lt <sourceport>|gt <sourceport>|
   ne <sourceport>}{<ipv6-destination-address/prefix-length>|any}
   {eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]

no ipv6 access-list extended <list-name> {deny|permit} {tcp|udp}
   {<ipv6-source-address/prefix-length>|any} {eq <sourceport>|
   lt <sourceport>|gt <sourceport>|
   ne <sourceport>}{<ipv6-destination-addr/prefix-length>|any}
   {eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.
deny	The IPv6 software extended access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The IPv6 software extended access-list permits packets that match the type, source, and destination filtering specified with this command.
any	For ICMP|IP The IPv6 software extended access-list matches any type of packet.

Parameter (cont.)	Description (cont.)
`ip`	For ICMP|IP The IPv6 software extended access-list matches only IP packets.
`icmp`	For ICMP|IP The IPv6 software extended access-list matches only ICMP packets.
`tcp`	For TCP/UDP The IPv6 software extended access-list matches only TCP packets.
`udp`	For TCP/UDP The IPv6 software extended access-list matches only UDP packets.
<ipv6-source-address/prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-destination-address/prefix-length>	Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`any`	Matches any IPv6 address.
<sourceport>	For TCP/UDP The source port number, specified as an integer between 0 and 65535.
<destport>	For TCP/UDP The destination port number, specified as an integer between 0 and 65535.
`icmp-type`	For ICMP|IP Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.
`eq`	For TCP/UDP Matches port numbers equal to the port number specified immediately after this parameter.
`lt`	For TCP/UDP Matches port numbers less than the port number specified immediately after this parameter.
`gt`	For TCP/UDP Matches port numbers greater than the port number specified immediately after this parameter.

Parameter (cont.)	Description (cont.)	
`ne`	For TCP/UDP Matches port numbers not equal to the port number specified immediately after this parameter.	
<icmp-type>	For ICMP|IP The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`log`	Logs the results.	

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

For backwards compatibility you can either create IPv6 extended access-lists from within this command, or you can enter `ipv6 access-list extended` followed by only the IPv6 extended access-list name. This latter (and preferred) method moves you to the `(config-ipv6-ext-acl)` prompt for the selected IPv6 extended access-list number, and from here you can configure the filters for this selected access-list.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example 1 [creating a list]

To add a new filter to the access-list named `my-list` that will reject incoming ICMP packets from `2001:0db8::0/64` to `2001:0db8::f/64`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# icmp 2001:0db8::0/64 2001:0db8::f/64
```

Example 2 [adding to a list]

To insert a new filter at sequence number `5` of the access-list named `my-list` that will accept ICMP type 8 packets from the `2001:0db8::0/64` network to the `2001:0db8::f/64` network, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 icmp 2001:0db8::0/64
                             2001:0db8::f/64
```

Example 3 [list with filter]

To create the access-list named `TK` to deny TCP protocols, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended TK deny tcp any eq
                14 any lt 12 log
```

Related Commands

ipv6 access-list extended proto (ipv6 access-list extended IP protocol filter)
ipv6 access-list extended TCP UDP filter)
show ipv6 access-list (IPv6 Software ACLs)
show running-config

ipv6 access-list extended proto

Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny packets with a specific value based on the IP protocol number specified.

The **no** variant of this command removes a specified IPv6 extended access-list with an IP protocol number.

Syntax

```
ipv6 access-list extended <list-name> {deny|permit}
   proto <ip-protocol>} {<ipv6-source-address/prefix>|any}
   {<ipv6-destination-address/prefix>|any} [log]

no ipv6 access-list extended <list-name> {deny|permit}
   proto <ip-protocol>{<ipv6-source-address/prefix>|any}
   {<ipv6-destination-address/prefix>|any} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
proto	The IP Protocol type specified by it protocol number <1-255>.
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**).
	Protocol Number
	1
	2
	3
	4
	5
	6
	8

Parameter (cont.)	Description (cont.)
<ip-protocol> (cont.)	**Protocol Number**
	9
	11
	17
	20
	27
	28
	29
	30
	33
	48
	50
	51
	54
	58
	59
	60
	88
	89
	97
	98
	108
	112
	134
	135
	136
	137
	138
	139-252
	253
	254
	255
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.

Parameter (cont.)	Description (cont.)
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`any`	Any destination address or remote address.
`log`	Log the results.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To create the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended ACL-1 deny proto 9
                2001:0db8:1::1/128 2001:0db8:f::1/128
```

To remove the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list extended ACL-1 deny proto
                10 2001:0db8:1::1/128 2001:0db8:f::1/128
```

Related Commands
ipv6 access-list extended (named)
(ipv6 access-list extended IP protocol filter)
show ipv6 access-list (IPv6 Software ACLs)
show running-config

(ipv6 access-list extended IP protocol filter)

Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol specified, to the current extended IPv6 access-list. If a sequence is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol filter entry, from the current extended IPv6 access-list. You can specify the ACL filter entry by entering either its sequence number, or its filter entry profile.

Syntax [ip|proto]

```
[<sequence-number>] {deny|permit} {ip|any|proto <ip-protocol>}
    {<ipv6-source-address/prefix>|any} {<ipv6-destination-address/
    prefix>|any} [log]

no {deny|permit} {ip|any|proto <ip-protocol>} {<ipv6-source-address/
    prefix>|any} {<ipv6-destination-address/prefix>|any} [log]

no [<sequence-number>]
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
ip	IP packet.
any	Any packet.
proto *<ip-protocol>*	The IP Protocol type specified by it protocol number <1-255>.
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority **www.iana.org/assignments/protocol-numbers**).
	Protocol Number
	1
	2
	3
	4
	5
	6
	8

Parameter(cont.)	Description(cont.)
<ip-protocol> (cont.)	**Protocol Number**
	9
	11
	17
	20
	27
	28
	29
	30
	33
	48
	50
	51
	54
	58
	59
	60
	88
	89
	97
	98
	108
	112
	134
	135
	136
	137
	138
	139-252
	253
	254
	255
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.

Parameter(cont.)	Description(cont.)
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`any`	Any destination address or remote address.
`log`	Log the results.

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To add a new ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5` rejecting the IPv6 packet from `2001:db8:1:1` to `2001:db8:f:1`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny ip 2001:db8:1::1/128
2001:db8:f::1/128
```

To remove the ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related Commands
ipv6 access-list extended (named)
show ipv6 access-list (IPv6 Software ACLs)
show running-config

(ipv6 access-list extended TCP UDP filter)

Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with a TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination port specified, to the current extended IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with a TCP or UDP source and destination port specified, from the current extended IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp} {<ipv6-source-address/
    prefix>|any} {eq <sourceport>|lt <sourceport>|gt <sourceport>|
    ne <sourceport>} {<IPv6-destination-address/prefix>|any}
    {eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]

no {deny|permit} {tcp|udp} {<ipv6-source-address/prefix>|any}
    {eq <sourceport>|lt <sourceport>|gt <sourceport>|
    ne <sourceport>}} {<IPv6-destination-address/prefix>|any}
    {eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
tcp	TCP packet.
udp	UDP packet.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
eq	Equal to.
lt	Less than.
gt	Greater than.
ne	Not equal to.
<sourceport>	The source port number, specified as an integer between 0 and 65535.
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Parameter(cont.)	Description(cont.)
<destport>	The destination port number, specified as an integer between 0 and 65535.
log	Log the results.

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any packet that has the specified source and destination IPv6 addresses and the specified TCP or UDP source and destination port. The parameter `any` may be specified if an address does not matter.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To add a new filter entry with sequence number `5` to the access-list named `my-list` to reject TCP packets from `2001:0db8::0/64` port `10` to `2001:0db8::f/64` port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny tcp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To add a new filter entry with sequence number `5` to the extended IPv6 access-list named `my-list` to reject UDP packets from `2001:0db8::0/64` port `10` to `2001:0db8::f/64` port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny udp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To remove the filter entry with sequence number `5` to the extended IPv6 access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related Commands **ipv6 access-list extended (named)**
show ipv6 access-list (IPv6 Software ACLs)
show running-config

ipv6 access-list standard (named)

This command configures an IPv6 standard access-list for filtering frames that permit or deny IPv6 packets from a specific source IPv6 address.

The **no** variant of this command removes a specified IPv6 standard access-list.

Syntax [list-name]

```
ipv6 access-list standard <ipv6-acl-list-name>

no ipv6 access-list standard <ipv6-acl-list-name>
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.

Syntax [deny|permit]

```
ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit}
   {<ipv6-source-address/prefix-length>|any} [exact-match]]

no ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit}
   {<ipv6-source-address/prefix-length>|any} [exact-match]]
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.
`deny`	The IPv6 software standard access-list rejects packets that match the type, source, and destination filtering specified with this command.
`permit`	The IPv6 software standard access-list permits packets that match the type, source, and destination filtering specified with this command.
<ipv6-source-address/prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
`any`	Matches any source IPv6 address.
`exact-match`	Exact match of the prefixes.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 standard access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 standard access-list when a match is encountered.

For backwards compatibility you can either create IPv6 standard access-lists from within this command, or you can enter `ipv6 access-list standard` followed by only the IPv6 standard access-list name. This latter (and preferred) method moves you to the `(config-ipv6-std-acl)` prompt for the selected IPv6 standard access-list, and from here you can configure the filters for this selected IPv6 standard access-list.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example To enter the IPv6 Standard ACL Configuration mode for the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)#
```

Related Commands
(ipv6 access-list standard filter)
show ipv6 access-list (IPv6 Software ACLs)
show running-config

(ipv6 access-list standard filter)

Use this ACL filter to add a filter entry for an IPv6 source address and prefix length to the current standard IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source address and prefix from the current standard IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [icmp]

```
[<sequence-number>] {deny|permit} {<ipv6-source-address/
   prefix-length>|any}

no {deny|permit} {<ipv6-source-address/prefix-length>|any}

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
<ipv6-source-address/prefix-length>	IPv6 source address and prefix-length in the form X:X::X:X/P.
any	Any IPv6 source host address.

Mode IPv6 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any IPv6 packet that has the specified IPv6 source address and prefix length. The parameter `any` may be specified if an address does not matter.

Note Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Examples To add an ACL filter entry with sequence number `5` that will deny any IPv6 packets to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# 5 deny any
```

To remove the ACL filter entry that will deny any IPv6 packets from the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no deny any
```

Alternately, to remove the ACL filter entry with sequence number `5` to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no 5
```

Related Commands

ipv6 access-list standard (named)
show ipv6 access-list (IPv6 Software ACLs)
show running-config

show ipv6 access-list (IPv6 Software ACLs)

Use the **show ipv6 access-list standard** command to display a specified standard named IPv6 access-list that has been defined using the **ipv6 access-list standard (named)** command.

Syntax

```
show ipv6 access-list standard <access-list-name>
```

Parameter	Description
`standard`	Named standard access-list.
`<access-list-name>`	Specify an IPv6 access-list name.

Mode User Exec and Privileged Exec

Example To show the ipv6 access-list specified with the name `acl_name` use the following command:

```
awplus# show ipv6 access-list standard acl_name
```

Output **Figure 39-1: Example output from the show ipv6 access-list standard command**

```
Named Standard IPv6 access-list name
  deny any
```

Related Commands

ipv6 access-list extended (named)
(ipv6 access-list extended IP protocol filter)
ipv6 access-list standard (named)
(ipv6 access-list extended TCP UDP filter)
(ipv6 access-list standard filter)

Chapter 40: Quality of Service (QoS) Introduction

Introduction 40.2
QoS Operations 40.2
QoS Packet Information 40.3
Link Layer QoS 40.3
Differentiated Services Architecture 40.4
The Differential Services Field 40.5
Processing Pre-Marked Packets 40.6
Applying QoS on Your Switch 40.7
Classifying Your Data 40.7
Class Maps 40.7
Policy Maps 40.10
Premarking and Remarking Your Traffic 40.11
CoS to Egress Queue Premarking 40.11
DSCP to Egress Queue Premarking 40.13
Policing (Metering) Your Data 40.15
Single-Rate Three-Color Policing 40.15
Two-Rate Three-Color Policing 40.16
Configuring and Applying a Policer 40.17
Remarking Your Data 40.18
Configuring the Egress Queues 40.19
Egress Queues and QoS markers 40.19
Egress Queue Commands Hierarchy 40.19
Egress Queue Shaping 40.21
Scheduling 40.21
Drop Mode 40.22
Storm Protection 40.24

Introduction

This chapter introduces the concept of Quality of Service (QoS) with particular reference to Allied Telesis switches running the AlliedWare Plus™ Operating System.

The concept of QoS is a departure from the original networking concept of treating all network traffic in the same way. Without QoS, all traffic types are equally likely to be dropped when a link becomes oversubscribed. With QoS, certain traffic types can be given preferential treatment. QoS is therefore a very useful tool both to control congestion and to meter or cap data in order to apply pre-agreed service levels.

Operationally, QoS is applied within the link and network layers. Functionally it provides the capability to intelligently transport your network traffic in order to provide stable and predictable end-to-end network performance.

Business benefits

Quality of Service mechanisms enable:

- network service providers to sell different levels of service to customers, based on what their customers require, and be confident in their ability to guarantee the reliable delivery of these services
- enterprise and educational organizations to actively manage and provide many services across one network, for example live video streaming and standard data services, with preferential treatment being given to mission-critical traffic
- network administrators to manage network congestion as network traffic levels increase and time-critical applications, such as streaming media, become more widely in demand by customers and organizations

QoS Operations

Quality of Service is typically based on how the switch performs the following functions:

- assigns priority to incoming frames (that do not already carry priority information)
- correlates prioritized frames with traffic classes, or maps frames to traffic classes based on other criteria
- correlates traffic classes with egress queues, or maps prioritized frames to egress queues
- provides minimum and maximum bandwidths for traffic classes, egress queues, and/or ports
- schedules frames in egress queues for transmission (for example, empty queues in strict priority or sample each queue)
- re-labels the priority of outgoing frames
- determines which frames to drop or re-queue if the network becomes congested
- reserves memory for switching/routing or QoS operation (for example, reserving buffers for egress queues or buffers to store packets with particular characteristics)

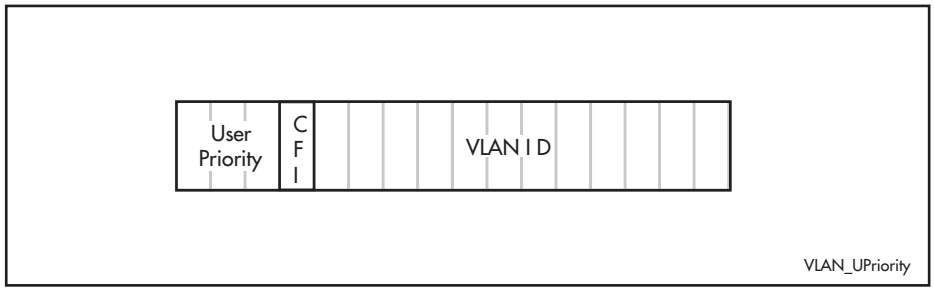
QoS Packet Information

Provision for QoS information to be embedded within the data fields exists within both the data link and network layer protocols. This information can then be used to assess the priority of the data and the resource preferences that need to be applied. The process of applying these service quality tags to your data is known as marking.

Link Layer QoS

Link layer frames entering a port may either be tagged or untagged. VLAN tagged frames contain the additional 802.1Q tag fields shown in **Figure 40-1** below. Located within the TCI is a three bit User Priority field. This field is specifically provided to attach QoS based priority information, often referred to as the Class of Service (CoS) field.

Figure 40-1: IEEE 802.1Q tagging



Appendix G of the IEEE Standard 802.1D provides some useful guidelines on applying priorities to 7 traffic types. These are summarized in the **Table 40-1** below.

Table 40-1: CoS traffic mapping guidelines

User Priority	Traffic Types
1	Background
2	Spare
0	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video <100 ms latency and jitter
6	Voice <10 ms latency and jitter
7	Network Control

On the switch you can use the **match cos** command to select frames that match a particular User Priority value and assign them to a particular class-map. You can then map these incoming frames to an egress queue. This facility enables you to accept frames that are already carrying meaningful priority information and automatically assign them to an appropriate egress queue. For example, you could decide to send frames with a User Priority value of 2 to queue 0. The process of assigning queues based on CoS tags is commonly known as “Pre-marking”.

Note

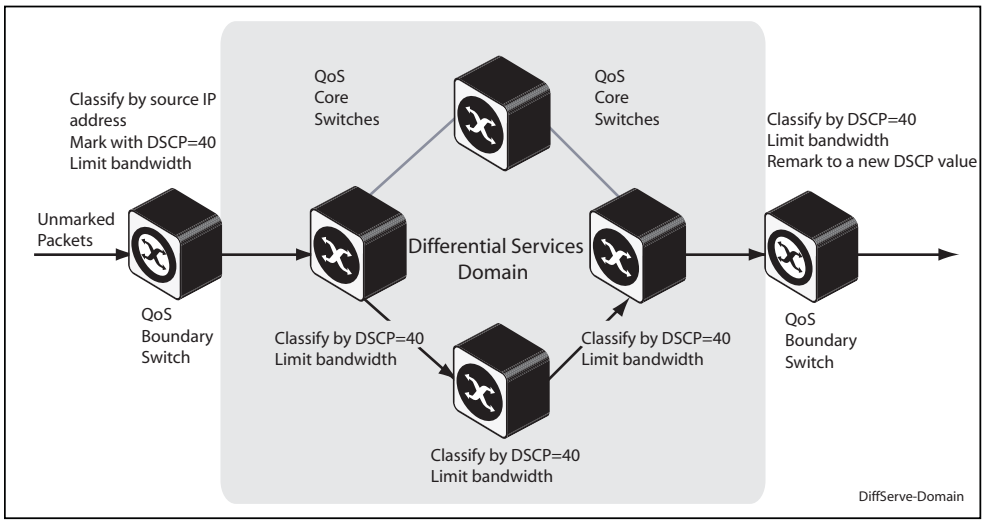
You configure the pre-marking steps on an ingress port. This process marks the data packets so that when they reach the egress port the decisions made during pre-marking can be applied in accordance with the configuration of the egress port.

Differentiated Services Architecture

Whilst a full description of the differential services model is outside the scope of this software reference, a brief introduction is provided. For further information, RFC 2475 provides an in depth definition of the architecture.

The basic differential services model envisages a multi router network within which common service qualities are applied. At the network boundary, *QoS Edge Routers* inspect the traffic and classify it into common service quality groups called Per Hop Behaviors (PHBs). A specific marker value called a Differential Services Code Point (DSCP) is added to the IP header of each packet, which allocates it to a PHB. *QoS Core Routers* within the network can then use the DSCP to decide on an appropriate service quality level to apply. When a network contains a consistently applied differential services code points DSCP it is referred as a Differential Services Domain (often shortened to DiffServe Domain). **Figure 40-2** shows a simple Differential Services Domain.

Figure 40-2: Differentiated Services Domain

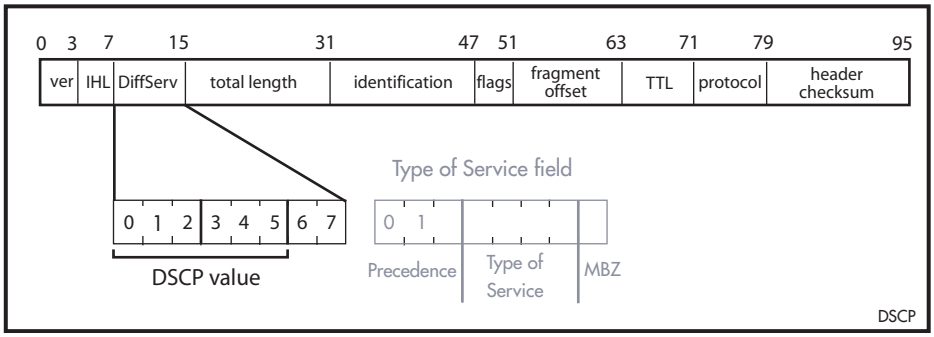


The Differential Services Field

Figure 40-3 shows an IP header containing a Differentiated Services field. The format of this redefined field is explained in RFC 2474; the main difference being that the old ToS field has been replaced by a 6 byte Differentiated Services Code Point (DSCP) field, which now provides for up to 64 defined values.

By applying this model only the QoS edge routers need to fully interrogate the incoming data packets; the QoS core routers are then relieved of this processing task and need only to inspect the DCSP before applying its appropriate forwarding, queuing, and shaping rules.

Figure 40-3: The DSCP bits of the DS field in the IPv4 header



On the switch you can use the **match dscp** command to select frames containing a particular DSCP value, and associate them with a particular class-map and policy-map.

Because the model offers considerable flexibility, and the mapping of traffic types to DCSPs is individual for each network, this locally applied definition is known as a *Differential Services Domain*. The previous section introduced the concept of a Per Hop (service quality) Behaviors or PHBs. RFC 2597 defines a specific PHB group called Assured Forwarding (AF). The AF PHB group provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. **Table 40-2** shows a list of recommended AF code points.

Table 40-2: Recommended DSCP code points

	(Lowest Priority) Class 1 (001xxxx)	Class 2 (010xxxx)	Class 3 (011xxxx)	(Highest Priority) Class 4 (100xxxx)
Low Drop Precedence	001010 AF11 Decimal 10	010010 AF21 Decimal 18	011010 AF31 Decimal 26	100010 AF41 Decimal 34
Medium Drop Precedence	001100 AF12 Decimal 12	010100 AF22 Decimal 20	011100 AF32 Decimal 28	100100 AF42 Decimal 36
High Drop Precedence	001110 AF13 Decimal 14	010110 AF23 Decimal 22	011110 AF33 Decimal 30	100110 AF43 Decimal 38

Processing Pre-Marked Packets

A logical question to ask at this point is: how does the QoS switch deal with data that arrives with a pre-existing service level tag such as a DSCP? As previously touched on, the differentiated services model envisages a network that comprises QoS boundary routers at its edge and QoS core routers in its core network.

At the network edge the QoS boundary routers filter the incoming data based on specific packet components. Based on this filtering each packet is assigned a DSCP value. This value will determine the service level (priority and queuing, for example) that will be applied.

Within the network core, the packet filtering required is reduced to simply reading the DSCP within each incoming packet, and applying the appropriate set of service levels. This relieves the core routers of the processing overhead of applying complex filtering to its high speed data streams.

Applying QoS on Your Switch

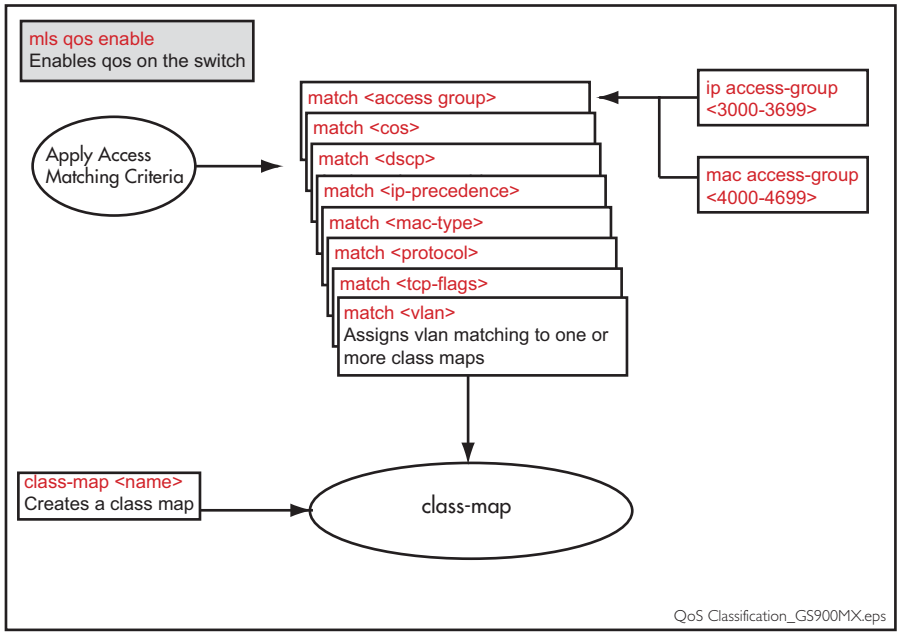
This section steps you through the various stages of QoS set-up and introduces the QoS commands and how to apply them.

Before you configure any QoS functions on your switch, first enable QoS by using the **mls qos enable** command.

Classifying Your Data

One of the early steps in setting up QoS on a network is planning and applying your classification rules. Classification is the process of **Filtering** and **Marking**. Filtering involves sorting your data into appropriate traffic types. Marking involves tagging the data so that downstream ports and routers can apply appropriate service policy rules. **Figure 40-4** illustrates the classifying process, and will be referred to in the examples that follow.

Figure 40-4: QoS classification process



At the premarking stage you can assign your data a particular priority level by giving it a link level user priority, see **"Link Layer QoS" on page 40.3**, or a network level DSCP **"Differentiated Services Architecture" on page 40.4**. You can also assign the data to a particular output (or egress) queue.

Class Maps

Class Maps are among the pivotal QoS components. They provide the means that associate the classified traffic with its appropriate QoS actions. They are the linking elements for the following functions:

- classification
- policy-mapping
- pre-marking

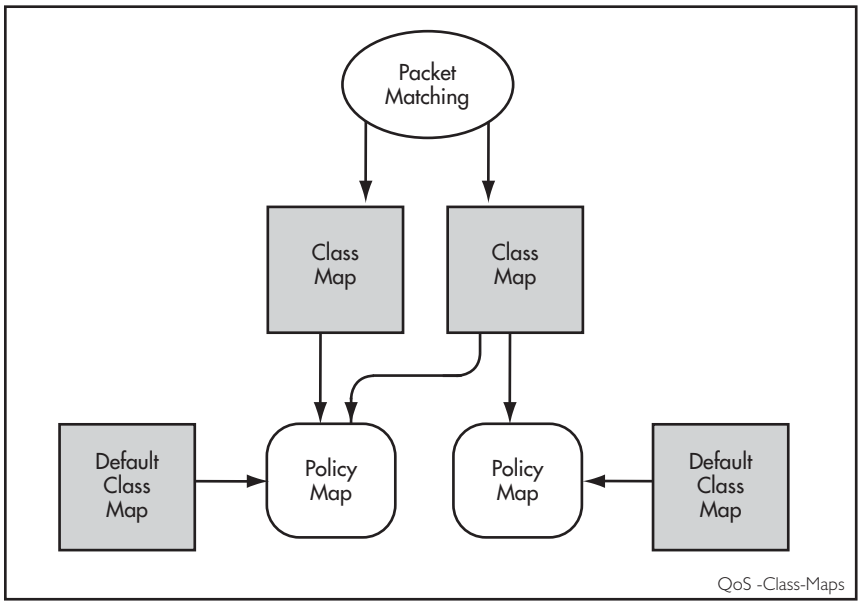
Figure 40-5 shows the relationship between a class-map and its associated functions. Note that the relationship between a class-map and a policy-map can be one-to-one or many-to-one. For information on policy-maps see the section, **"Policy Maps" on page 40.10**.

Note

If a conflict occurs between the settings in two class-maps, priority will be applied to the class-map that was created first.

An example of such a conflict is the arrival of a packet that meets the classification requirements of two class-maps each configured to the same policy-map and set to apply different priority settings to the packet.

Figure 40-5: Relationship between a class-map and its associated functions



Creating a class-map

To create a class-map, use the **class-map** command on page 41.3.

This example creates a class-map called **video-traffic** and another called **data-traffic**:

```
awplus# configure terminal
awplus(config)# class-map video-traffic
awplus(config-cmap)# exit
awplus(config)# class-map data-traffic
awplus(config-cmap)#
```

Creating and configuring default class-maps

These (automatically created) default class-maps serve as the means to specify the action that will apply to all unclassified data, i.e. all data within a policy-map that is not captured by any of the applied match commands that are applied to the policy-map by its class-maps.

Each time a new policy-map is created a new class-map called "default" is also automatically created and assigned to the new policy-map. You can configure any of the default class-maps by using the **default-action** command on page 41.5

To set the default class-map for the policy-map **p-map1** to have the action of `deny`:

```
awplus# config
awplus(config)# policy-map p-map1
awplus(config-pmap)# default-action deny
```

Applying a match command to a class-map

To apply a matching filter to a class-map use one of the match commands.

This example creates a filter to select VLAN 5 traffic and applies this filter to the class-map named **video-traffic**.

```
awplus# config terminal
awplus(config)# class-map video-traffic
awplus(config-cmap)# match vlan 5
```

Associating a class-map with a policy-map

To associate a class-map with a policy-map, use the **class** command on page 41.2.

Note A maximum of 128 class-maps may be attached to each policy-map.

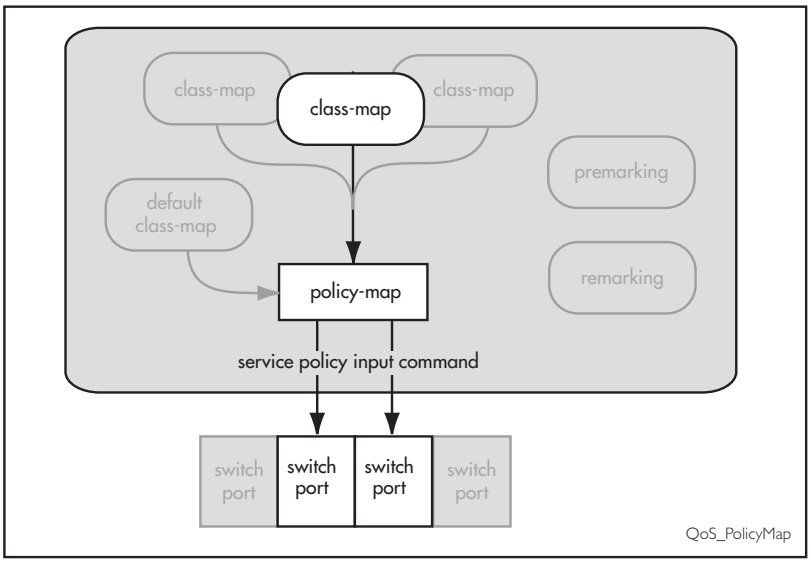
The following example creates a policy-map called **policy-one**, and associates it with the class-maps named **video-traffic**, and **database-traffic**:

```
awplus# configure terminal
awplus(config)# policy-map policy-one
awplus(config-pmap)# class video-traffic
awplus(config-pmap-c)# exit
awplus(config-pmap)# class database-traffic
awplus(config-pmap-c)#
```

Policy Maps

Policy maps are the means by which you apply your class-map properties to physical switch ports. **Figure 40-6 on page 40.10** illustrates this concept. Note that a policy-map can be assigned to several ports, but a port cannot have more than one policy-map assigned to it.

Figure 40-6: Policy maps and related entities



To create and name a new policy-map you use the **policy-map** command on page 41.28.

To create a policy-map called `pmap1` use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
```

Having created the policy-map `pmap1` we can use the **class** command on page 41.2 to assign it to one or more class-maps. Since we created the class-maps `video-traffic` and `office-traffic` earlier in this chapter, we can now attach the policy-map `pmap1` to both class-maps.

Use the **class** command to assign the policy-map `pmap1` to the class-maps `video-traffic` and `office-traffic`:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class video-traffic
awplus(config-pmap-c)# exit
awplus(config-pmap)# class office-traffic
awplus(config-pmap-c)#
```

Premarking and Remarking Your Traffic

Premarking relates to adding QoS markers to your incoming data traffic before it is metered (policed). Remarking is the same process when applied after metering. Network switches will often be configured with two different premarking profiles, one for the QoS edge switches and another for the QoS core switches. This situation would apply if you are operating DSCP domains.

QoS markers can be applied at both the link layer (within the CoS field), and at the network layer (within the DSCP field). For more information on this topic see **"QoS Packet Information" on page 40.3**.

For boundary QoS switches

Traffic entering QoS boundary switches is unlikely to contain pre-existing QoS tagging. In this case, you can:

- Assign a CoS tag to data associated with a particular class-map.
- Use the **trust dscp** command to enable the mls qos map premark DSCP map. This map enables you to change the DSCP tag and also map the tag to an egress port queue, a CoS value, or both. At the premarking stage you can set this mapping using the command **mls qos map premark-dscp to**. After policing, you can then use the **remark-map** command to change the DCSP based on the packet's bandwidth class, or remap the existing bandwidth class, to a new value.

For an untagged packet, if no other mapping is applied and the packet is untagged, (i.e. in the absence of any other queue selection) traffic will be sent to queue 2.

For core QoS switches

Traffic entering ports within the QoS core network will almost certainly contain some pre-existing QoS tagging. Where this is the case, you can:

- Map the CoS tag to an egress queue. You can do this either for the whole switch or for specific ports via their assigned policy-maps. See **"CoS to Egress Queue Premarking" on page 40.11**.
- Map the DSCP tag to an output queue. You can do this either for the whole switch or for specific ports via their assigned policy-maps.
- Remap incoming data DSCP or CoS tags to values that are more appropriate for a particular switch or network.
- Assign bandwidth classes for your packets, based on the incoming DSCP. See **"DSCP to egress queue premarking commands" on page 40.13**.

CoS to Egress Queue Premarking

If you are using CoS tagging for your QoS functions, your traffic is likely to be either entering the switch with a pre-existing CoS tag, or will have appropriate tags attached via your class-maps and policy-maps. You can now mark the data for a particular egress queue, which will take effect when the data reaches its output port. There are two fundamental methods of applying CoS tagged packets to egress queues:

1. Apply a global mapping of CoS tags to egress queues for all ports.
2. Apply a CoS to egress queue mapping for the class-map / policy-map. This mapping - which forms part of the policy-map - is applied at an input port, but will take effect at the packet's destination output port. Note that this procedure takes priority over that described in method (1) above.

These methods and their related commands will be now be described in greater detail.

Note

Where a packet contains both a CoS and a DSCP field, and each field maps to a different class-map; the switch will apply a priority that is based on the date that the class-map was added to the policy-map; the earlier the date, the higher the priority.

Mapping CoS tags to traffic types

The command **mls qos map cos-queue to** enables you to create a switch-wide mapping of CoS values to egress queues. The default mappings for this command are:

```
COS :            0 1 2 3 4 5 6 7
--------------------------------
QUEUE:           2 0 1 3 4 5 6 7
```

These mappings match the CoS guidelines documented in Annex H.2 of ANSI/IEEE 802.1D 1988 Edition. Table H-15 on page 355 of the standard shows a table of user priorities for specific traffic types. **Table 40-3** shows an adapted version of the ANSI/IEEE table.

Table 40-3: Traffic type guidelines

User Priority (egress queue)	CoS Value	Acronym	Traffic type	Internal Traffic Queue Defaults
0 (lowest)	1	BK	Background	
1	2	-	Spare	
2	0	BE	Best Effort	Default
3	3	EE	Excellent Effort	
4	4	CL	Controlled Load	
5	5	VI	"Video," <100 ms latency and jitter	
6	6	VO	"Voice," <10 ms latency and jitter	EPSR-Management BPDU ARP-Requests
7 (highest)	7	NC	Network Control	Stack Management

CoS settings for VCStack stack operation

In general you can apply the same principles when configuring QoS on a VCStack as you would for single switch; however there are a few specific changes that you will need to make.

Switches within a VCStack exchange their stack management information and user data over their high speed inter-stacking links. The stack management information is pre-assigned to the egress queue 7. This is the highest value queue, and (in a stacked configuration) its traffic should not be shared with any user data. However, any CoS tagging of 7 applied to the incoming data will automatically be assigned to queue 7 as it crosses the internal stacking links. You will therefore need to reconfigure your CoS to Queue settings to ensure that no user data is sent to queue 7.

To prevent this from happening, we recommend that you make appropriate changes to your queue settings (mappings) to reflect the stacking requirement previously described. For more information on this topic, see **"Mapping CoS tags to traffic types" on page 40.12**.

This process should include (but not be limited to) running the following command to ensure that any remaining user still carrying a CoS 7 tag will be mapped to egress queue 6.

To remap priority CoS traffic to egress queue 6, run the following command.

```
awplus# config terminal
awplus(config)# mls qos map cos-queue 7 to 6
```

DSCP to Egress Queue Premarking

If you are using DSCP tagging for your QoS functions, your traffic is likely to be entering the switch either with a pre-existing DSCP tag, or will have appropriate DSCP tags attached via your class-maps and policy-maps. You can now mark the data for a particular egress queue, which will take effect when the data reaches its output port.

If your switch forms part of a DSCP domain, you can adapt the steps in this section to apply the mappings and settings to match the standards you have selected for the domain. This mapping - which forms part of the policy-map - is applied at an input port, but will take effect at the packet's destination output port.

DSCP to egress queue premarking commands

A number of commands can be used for mapping DSCP tags. Where these conflict, the switch applies a pre-defined set of priorities. **Table 40-4** lists these priorities in order (lowest priority first).

Where a packet that contains both CoS and a DSCP fields and each field maps to a different class-map / policy-map, the switch will apply a priority based on the creation date of class-maps - the earlier the creation date, the higher the priority priorities.

Table 40-4: DSCP mapping commands in hierarchical order

Command	Function
trust dscp	Setting the trust dscp enables the **mls qos map premark-dscp to** command to apply. See **"Setting the Trust DSCP map" on page 40.14**.
mls qos map premark-dscp to	With the trust dscp set, this command applies a remapping table whose values include the dscp and egress queues.

Setting the Trust DSCP map

The Trust DSCP mapping table assigns a new set of QoS values for a DSCP value supplied as table input. To configure this table you use the **mls qos map premark-dscp to** command.

Table 40-5: Drop probability table

Table Input	---------- Table Output ----------			
Existing DSCP	New DSCP Value	New CoS Value	New Queue No	New BW Class green yellow red

The Trust DSCP map provides the highest priority of all the pre-marking controls. To apply this table you must first apply the trust setting by using the **trust dscp** command.

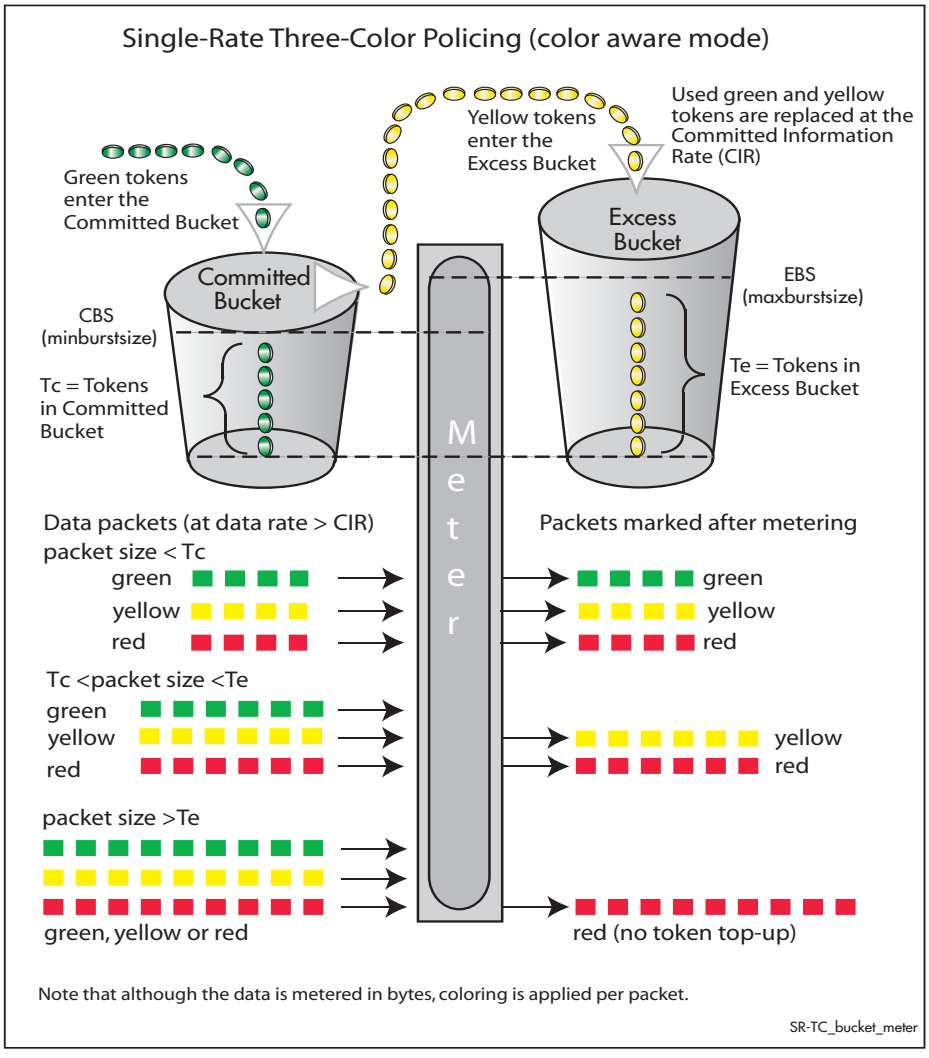
Policing (Metering) Your Data

Once you have set-up your classification and created your class-maps, you can start conditioning your traffic flows. One tool used for traffic conditioning is the policer (or meter). The principle of policing is to measure the data flow that matches the definitions for a particular class-map; then, by selecting appropriate data rates, allocate the flows into one of three categories: Red, Yellow, or Green. You then decide what action to apply to the colored data.

Single-Rate Three-Color Policing

This policing method is based on that defined in RFC 2697. The principle of single-rate three-color policing is shown in **Figure 40-7**. For a given class-map, a meter monitors both the token count in the buckets, and the input data flow.

Figure 40-7: Single-rate three-color policing



Each byte entering the meter is paired with a token in one of the buckets, and a token is removed as each byte is accepted. If the input data rate is the same as the CIR then the data passes through the port at the same rate as its bucket fills. Hence the bucket level remains constant. In this model, the data buffer is represented by two data buckets. You can specify the CIR using the **police single-rate action** command.

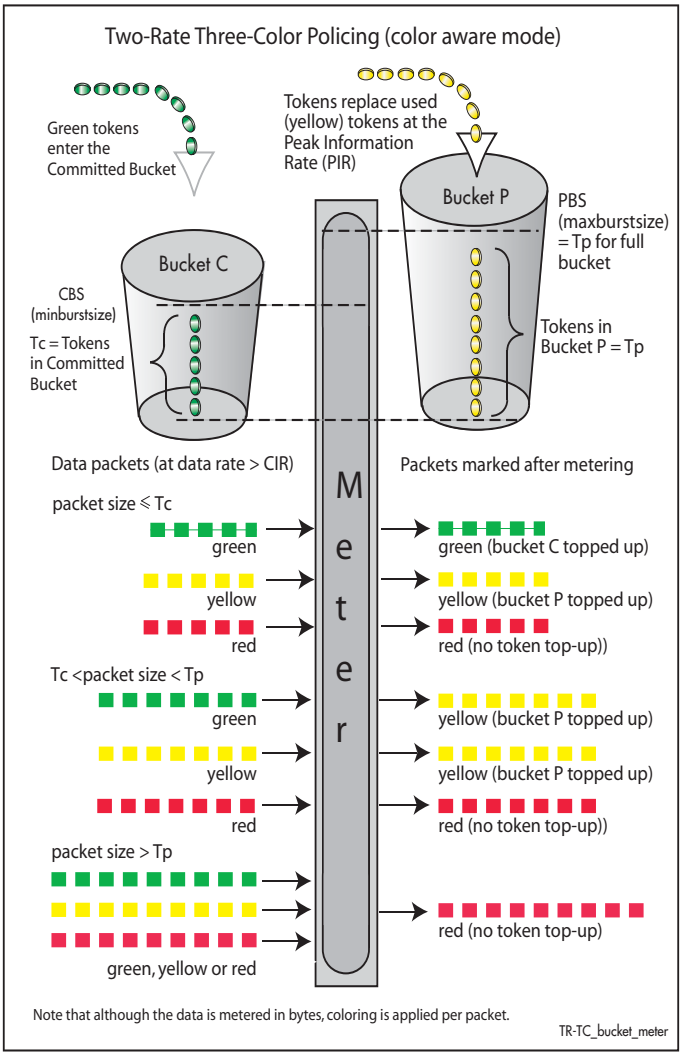
Initially both buckets have their full token count. A surge of data exceeding the CIR will begin to empty the bucket. As the data and tokens are paired, data bytes that match tokens below the CBS level are marked green, those that are between CBS and EBS will be marked yellow, and those that are above EBS are marked red.

Note that although the data is metered per byte, the color marking process is applied per packet. This means that if there were only sufficient tokens available to match part of a packet, then the whole packet would be marked red. Then, depending on the **action** parameter of the **police single-rate action** command, the whole packet will be either dropped or forwarded. In either situation, the red-marked packet will leave the bucket counts unchanged.

Two-Rate Three-Color Policing

This policing method is based on that defined in RFC 2698. The principle of two-rate three-color policing is shown in **Figure 40-8**.

Figure 40-8: Two-rate three-color policing



For a given class-map, the meter monitors the token count in both buckets, and the input data flow. Initially tokens enter both buckets until full. As the data enters a port, the meter pairs each byte to a token in one of the buckets, then removes a token from the appropriate bucket. Bucket C is topped up with tokens at the Committed Information Rate (CIR), and bucket P is topped up at the Peak Information Rate (PIR).

When data enters the port at the CIR, the bucket fills at the same rate as the incoming data, thus the token count in bucket C remains constant. Similarly, if data enters the port at the PIR, then the token count in bucket P remains constant. You can specify the CIR and the PIR by using the **police twin-rate action** command. The function of this command is explained in the section **"Configuring and Applying a Policer" on page 40.17**.

A surge of data exceeding the CIR will begin to empty bucket C. If bucket C empties to a point where it has insufficient tokens to match to an incoming data packet, then the data packet will be marked yellow. The data will now be measured against the level in bucket P and tokens will be removed from this bucket to match the incoming data. If the incoming data rate drops to less than the CIR then the data will continue to be marked yellow until the level in bucket C has had a chance to fill, whereupon it will be marked *green*.

If the incoming data is greater than the PIR, then bucket P begins to empty. If bucket P empties to a point where it has insufficient tokens to match to an incoming data packet, then the data packet will be marked *red*. In this situation no tokens are removed from either bucket.

Note that although the data is metered per byte, the color marking process is applied per packet. This means that if there were only sufficient tokens available to match part of a packet, then the whole packet would be marked red. Then, depending on the **action** parameter of the **police twin-rate action** command, the whole packet will be either dropped, or marked and forwarded. In either situation, the red marked packet will leave the bucket counts unchanged.

Configuring and Applying a Policer

The previous section showed how the policer works and how to select either the single rate or twin rate action. To apply a policy to class-maps:

- Select your policy-map and class-map from the command prompt, then enter either the **police single-rate action** command or the **police twin-rate action** command whilst selecting the appropriate command parameters.

This will apply the command to the selected class-map. By running this command several times, each for a different class-map, you can apply separate meter settings to each class-map.

Remarking Your Data

The remarking process enables you to change the QoS tagging and queue assignments from data that has already been marked by the policer. To do this you fill entries in the remarking table by using the **remark-map** command on page 41.30. In order to remark your data ensure that the **action** parameter of either the **police single-rate action** or the **police twin-rate action** is set to **remark-transmit**.

The following table shows the remarking options.

Table 40-6: Remarking table

BANDWIDTH CLASS		
Green	New DSCP	New bandwidth class (Red, Yellow, or Green)
Yellow	New DSCP	New bandwidth class (Red, Yellow, or Green)
Red	New DSCP	New bandwidth class (Red, Yellow, or Green)

Example Traffic presently marked Yellow is to be assigned a new DSCP value of 20:

Table 40-7: Remarking table example

BANDWIDTH CLASS		
Yellow	New DSCP = 20	Bandwidth class unchanged

To configure this setting, you would enter the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class yellow to
new-dscp 20
```

Further remarking can be achieved by using the **remark new-cos** command on page 41.32. This command enables you to configure and remark either or both the CoS flag in the data packet, and the input into the CoS to queue map thus changing the destination egress queue.

Configuring the Egress Queues

Previous sections have explained the ingress functions. These include how the incoming data can be classified and marked according to its priority and allocated to an egress queue, then finally how metering and remarking is applied. At this point the data then flows across the switch to its destination egress port where its transit to the egress queues is controlled.

The means by which data is applied to the egress queues is dependent on three functions:

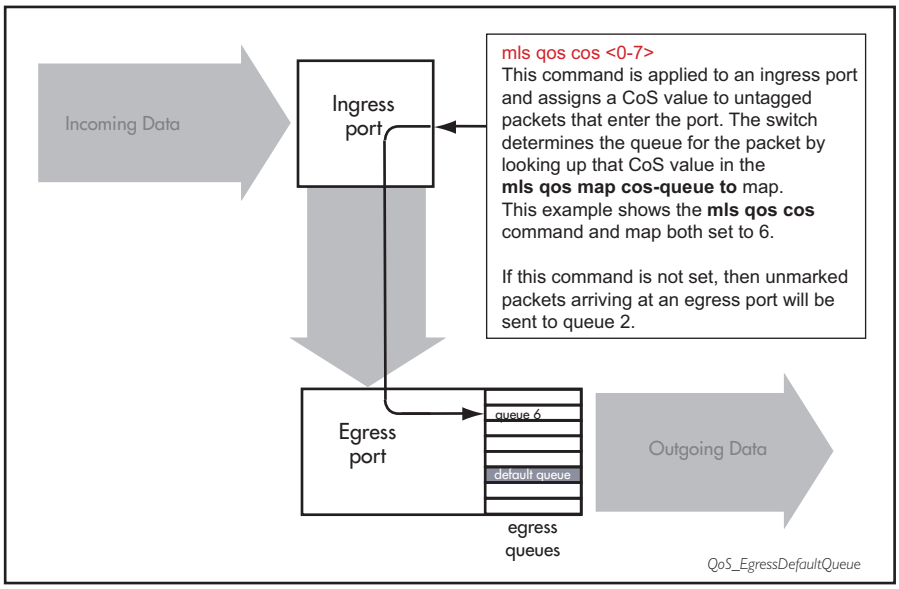
- Egress queue and QoS markers that are set within each data packet
- Egress controls that are applied to the whole switch
- Egress controls that are applied to each individual switch port

Egress Queues and QoS markers

Once the data packets have been appropriately filtered, classified, policed, and remarked, they travel across the switch's internal paths carrying their assigned QoS tag markers such as their priority, class and destination queues. For more details on ingress data marking, refer to the earlier sections of this chapter. At the egress port these markers are read and used to determine which queues each data packet will be forwarded to, and the priorities that will be applied.

There are eight egress queues allocated to each egress port. The egress queue that a particular packet passes through is determined by either the configuration of the switch, or by the markers contained within the packet itself.

Figure 40-9: Default egress queue



Egress Queue Commands Hierarchy

The destination queue that any one packet will take depends on the markers within the packet, and the way the queuing commands have been set. Also, some queuing commands will override others. Here is how the switch prioritizes its queuing commands.

Imagine a packet entering an ingress port then traveling through the switch fabric to reach its appropriate egress port. In this situation the following hierarchy will apply:

1. If the packet enters an egress port carrying no QoS markers and no QoS queuing commands have been set on the switch, then the packet will exit the port via queue number 2.

2. This default situation can be overridden by the **mls qos cos** command, which assigns a CoS value to untagged packets that enter a port. The switch determines the queue for the packet by looking up that CoS value in the **mls qos map cos-queue to** map.

3. If the packet contains a CoS value and arrives at an egress port with no other configuration applying, the switch determines the queue for the packet by looking up that CoS value in the **mls qos map cos-queue to** map.

4. The above CoS and queue settings can be overridden by the **remark new-cos** command. This command lets you change the CoS value for packets that match a given class-map, and therefore lets you change the queue for those packets.

Egress Queue Shaping

This section is concerned with how the egress queues are cleared.

Scheduling

The scheduler determines how packets in the egress port queues are serviced. Two servicing methods can be applied:

- strict priority
- weighted round robin (WRR)

Strict priority servicing

By default, all queues on all ports are serviced in a strict priority order. This means that the highest numbered priority queue (queue 7) is emptied first; then when it is completely empty, the next highest priority queue is processed, and so on. Thus, for a strict priority queue to be processed, all higher priority queues must be empty.

Strict priority servicing is the default setting; however if your system is configured for weighted round robin (WRR), you can return it to priority queuing by using the commands shown in the following example.

To return queue 2 of `port1.0.1` from WRR servicing to strict priority queuing, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# priority-queue 2
```

Weighted round robin servicing

The following examples show how to configure round robin servicing.

Example To configure a wrr-queue by applying a weighting value of 6 to queues 0 and1:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue weight 6 queues 0 1
```

Example In this example port 1.0.1 has queues configured as follows:

- queues 6 and 7 are configured strict priority
- queues 3 and 4 are configured as WRR with weighting values of 6
- queue 5 is configured as WRR with weighting values of 12
- queues 0, 1 and 2 are configured as WRR with weighting values of 4

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# priority-queue 6 7
awplus(config-if)# wrr-queue weight 6 queues 3 4
awplus(config-if)# wrr-queue weight 12 queues 5
awplus(config-if)# wrr-queue weight 4 queues 0 1 2
```

In this example, the queues are processed as follows:

1. Queue 7 is processed first.
2. If queue 7 is empty, Queue 6 is processed next.
3. If queues 6 and 7 are empty, queue 5 is processed next.
4. If queue 5 is empty, queues 3 and 4 are processed with equal weighting.

Drop Mode

The drop mode sets the limits for packets in the egress queues and determines how packets will be dropped if the queues become congested. The switch supports the tail drop mode and is pre-configured with the following settings:

Data packets will be dropped per color at the following buffer usage:

Red at 60%, Yellow at 80%, and Green at 100%.

These settings cannot be reconfigured.

Tail drop

In this drop mode each egress queue is configured with a maximum threshold value. This value represents the point where the egress buffer queues are full and the egress port must start dropping data. The port does this by dropping data packets destined for the full queue on a “last in first dropped” basis. This enables the port to clear its data already queued for egress.

If a reliable transport protocol, such as TCP is used, this data should be retransmitted, but at a slower rate due to lack of returning “acknowledgments”.

Storm Protection

Storm protection uses QoS mechanisms to classify on traffic likely to cause a packet storm (broadcast and multicast). Unless you are running an enhanced storm protection feature such as Loop Protection, the per-port storm protection mechanism simply discards any traffic over the configured limit. However, with QoS storm protection, several actions are possible when a storm is detected:

- You can disable the port physically.
- You can disable the port logically.
- You can disable the port for a particular VLAN.

To enable the policy-based storm protection, use the **storm-protection** command on page 41.47.

Storm protection is activated as soon as a port is enabled, before the port forwards frames.

When a storm is detected on a port, a message is automatically recorded in the log, and you can configure an SNMP trap to signal that a port has been disabled. When a storm is detected on a trunk or port group, the entire trunk or port group is disabled.

The following table explains the basic concepts involved with storm protection.

Concept	Description
Window	The frequency at which traffic is measured to determine whether storm protection should be activated.
Rate	The amount of traffic per second that must be exceeded before the switch takes the configured action.
Action	What the switch does when it detects a storm on a port.
Timeout	The length of time the port remains disabled after a port has been disabled due to a packet storm.

To set the action to take when triggered by QoS Storm Protection (QSP), use the **storm-action** command on page 41.45.

To set the time to re-enable the port once disabled by QSP, use the **storm-downtime** command on page 41.46.

Chapter 41: QoS Commands

Command List 41.2
class 41.2
class-map 41.3
clear mls qos interface policer-counters 41.4
default-action 41.5
description (QoS policy-map) 41.6
egress-rate-limit 41.7
match access-group 41.8
match cos 41.9
match dscp 41.10
match eth-format protocol 41.11
match ip-precedence 41.14
match mac-type 41.15
match tcp-flags 41.16
match vlan 41.17
mls qos cos 41.18
mls qos enable 41.19
mls qos map cos-queue to 41.20
mls qos map premark-dscp to 41.21
no police 41.23
police single-rate action 41.24
police twin-rate action 41.26
policy-map 41.28
priority-queue 41.29
remark-map 41.30
remark new-cos 41.32
service-policy input 41.34
show class-map 41.35
show mls qos 41.36
show mls qos interface 41.37
show mls qos interface policer-counters 41.39
show mls qos interface queue-counters 41.40
show mls qos interface storm-status 41.41
show mls qos maps cos-queue 41.42
show mls qos maps premark-dscp 41.43
show policy-map 41.44
storm-action 41.45
storm-downtime 41.46
storm-protection 41.47
storm-rate 41.48
storm-window 41.49
trust dscp 41.50
wrr-queue disable queues 41.51
wrr-queue weight queues 41.52

Command List

This chapter provides an alphabetical reference for Quality of Service commands. For more information, see **Chapter 40, Quality of Service (QoS) Introduction** and **Chapter 36, Access Control Lists Introduction**.

class

Use this command to associate an existing class-map to a policy or policy-map (traffic classification), and to enter Policy Map Class Configuration mode to configure the class-map.

Use the **no** variant of this command to delete an existing class-map.

For more information on class-maps and policy-maps, see the following sections:**"Class Maps" on page 40.7** and **"Policy Maps" on page 40.10**.

Note that if your class-map does not exist, you can create it by using the **class-map** command.

Syntax

```
class {<name>|default}
no class <name>
```

Parameter	Description
<name>	Name of the (already existing) class-map.
`default`	Specify the default class-map.

Mode Policy Map Configuration

Example The following example creates the policy-map `pmap1`(using the policy-map command), then associates this to an already existing class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)#
```

Related Commands **class-map**
policy-map

class-map

Use this command to create a class-map.

Use the **no** variant of this command to delete the named class-map.

Syntax

```
class-map <name>
no class-map <name>
```

Parameter	Description
<name>	Name of the class-map to be created.

Mode Global Configuration

Example This example creates a class-map called `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)#
```

clear mls qos interface policer-counters

Resets an interface's policer counters to zero. This can either be for a specific class-map or for all class-maps.

Syntax

```
clear mls qos interface <port> policer-counters
   [class-map <class-map>]
```

Parameter	Description
<port>	The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).
`class-map`	Select a class-map.
<class-map>	Class-map name.

Mode Privileged Exec

Example To reset the policy counters to zero for all class-maps for `port1.0.1`, use the command:

```
awplus# clear mls qos interface port1.0.1 policer-counters
```

Related Commands show mls qos interface policer-counters

default-action

Sets the action for the default class-map belonging to a particular policy-map. The action for a non-default class-map depends on the action of any ACL that is applied to the policy-map.

The default action can therefore be thought of as specifying the action that will be applied to any data that does not meet the criteria specified by the applied matching commands.

Use the **no** variant of this command to reset to the default action of 'permit'.

Syntax

```
default-action [permit|deny|send-to-cpu|copy-to-cpu|copy-to-mirror|
   send-to-mirror]

no default-action
```

Parameter	Description
`permit`	Packets to permit.
`deny`	Packets to deny.
`send-to-cpu`	Specify packets to send to the CPU.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`send-to-mirror`	Specify packets to send to the mirror port.

Default The default is '`permit`'.

Mode Policy Map Configuration

Examples To set the action for the default class-map to `deny`, use the command:

```
awplus(config-pmap)# default-action deny
```

To set the action for the default class-map to `copy-to-mirror` for use with the **mirror interface** command, use the command:

```
awplus(config-pmap)# default-action copy-to-mirror
```

Related Commands **mirror interface**

description (QoS policy-map)

Adds a textual description of the policy-map. This can be up to 80 characters long.

Use the **no** variant of this command to remove the current description from the policy-map.

Syntax

```
description <line>
no description
```

Parameter	Description
<line>	Up to 80 character long line description.

Mode Policy Map Configuration

Example To add the description, VOIP traffic, use the commands:

```
awplus(config-pmap)# description VOIP traffic
```

egress-rate-limit

Sets a limit on the amount of traffic that can be transmitted per second from this port.

Use the **no** variant of this command to disable the limiting of traffic egressing on the interface.

Syntax

```
egress-rate-limit <bandwidth>
no egress-rate-limit
```

Parameter	Description
<bandwidth>	Bandwidth <1-10000000 units per second> (usable units: k, m, g). The egress rate limit can be configured in multiples of 64kbps. If you configure a value that is not an exact multiple of 64kbps, then the value will be rounded up to the nearest higher exact multiple of 64kbps. The minimum is 64 Kb. The default unit is Kb (**k**), but Mb (**m**) or Gb (**g**) can also be specified. The command syntax is not case sensitive, so a value such as 20m or 20M will be taken to mean 20 megabits.

Mode Interface Configuration

Examples To enable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit 64k
% Egress rate limit has been set to 64 Kb
```

To disable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit
```

match access-group

Use this command to define match criterion for a class-map.

Syntax

```
match access-group {<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
no match access-group {<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
```

Parameter	Description
<hw-IP-ACL>	Specify a hardware IP ACL number in the range <3000-3699>.
<hw-MAC-ACL>	Specify a hardware MAC ACL number in the range <4000-4699>.
<hw-named-ACL>	Specify the hardware named ACL.

Mode Class Map Configuration

Usage First create an access-list that applies the appropriate permit/deny requirements. Then use the **match access-group** command to apply this access-list for matching to a class-map. Note that this command will apply the access-list matching only to *incoming* data packets.

Examples To configure a class-map named `cmap1` with one match criterion: `access-list 3001`, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 permit ip any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3001
```

To configure a class-map named `cmap2` with one match criterion: `access-list 3001`, which allows MAC traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit any any
awplus(config)# class-map cmap2
awplus(config-cmap)# match access-group 4001
```

To configure a class-map named `cmap3` with one match criterion: `access-list hw_acl`, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware hw_acl
awplus(config-ip-hw-acl)# permit ip any any
awplus(config)# class-map cmap3
awplus(config-cmap)# match access-group hw_acl
```

Related Commands class-map

match cos

Sets the CoS for a class-map to match on.

Use the **no** variant of this command to remove CoS.

Syntax

```
match cos <0-7>
no match cos
```

Parameter	Description
<0-7>	Specify the CoS value.

Mode Class Map Configuration

Examples To set the class-map's CoS to `4`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match cos 4
```

To remove CoS from a class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match cos
```

match dscp

Use this command to define the DSCP to match against incoming packets.

Use the **no** variant of this command to remove a previously defined DSCP.

Syntax

```
match dscp <0-63>
no match dscp
```

Parameter	Description
<0-63>	Specify DSCP value (only one value can be selected).

Mode Class Map Configuration

Usage Use the **match dscp** command to define the match criterion after creating a class-map.

Examples To configure a class-map named `cmap1` with criterion that matches IP DSCP 56, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match dscp 56
```

To remove a previously defined DSCP from a class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match dscp
```

Related Commands class-map

match eth-format protocol

This command sets the Ethernet format and the protocol for a class-map to match on.

Select one Layer 2 format and one Layer 3 protocol when you issue this command.

Use the **no** variant of this command to remove the configured Ethernet format and protocol from a class-map.

Syntax `match eth-format <layer-two-format> protocol <layer-three-protocol>`

`no match eth-format protocol`

Parameter	Description
<layer-two-formats>	
`802dot2-tagged`	802.2 Tagged Packets (enter the parameter name).
`802dot2-untagged`	802.2 Untagged Packets (enter the parameter name).
`ethii-tagged`	EthII Tagged Packets (enter the parameter name).
`ethii-untagged`	EthII Untagged Packets (enter the parameter name).
`netwareraw-tagged`	Netware Raw Tagged Packets (enter the parameter name).
`netwareraw-untagged`	Netware Raw Untagged Packets (enter the parameter name).
`snap-tagged`	SNAP Tagged Packets (enter the parameter name).
`snap-untagged`	SNAP Untagged Packets (enter the parameter name).
<layer-three-protocols>	
`<word>`	A Valid Protocol Number in hexidecimal.
`any`	Note that the parameter “any” is only valid when used with the netwarerawtagged and netwarerawuntagged protocol options.
`sna-path-control`	Protocol Number 04 (enter the parameter name or its number).
`proway-lan`	Protocol Number 0E (enter the parameter name or its number).
`eia-rs Protocol`	Number 4E (enter the parameter name or its number).
`proway Protocol`	Number 8E (enter the parameter name or its number).
`ipx-802dot2`	Protocol Number E0 (enter the parameter name or its number).
`netbeui`	Protocol Number F0 (enter the parameter name or its number).
`iso-clns-is`	Protocol Number FE (enter the parameter name or its number).

Parameter(cont.)	Description(cont.)
xdot75-internet	Protocol Number 0801(enter the parameter name or its number).
nbs-internet	Protocol Number 0802 (enter the parameter name or its number).
ecma-internet	Protocol Number 0803 (enter the parameter name or its number).
chaosnet	Protocol Number 0804 (enter the parameter name or its number).
xdot25-level-3	Protocol Number 0805 (enter the parameter name or its number).
arp Protocol	Number 0806 (enter the parameter name or its number).
xns-compat	Protocol Number 0807 (enter the parameter name or its number).
banyan-systems	Protocol Number 0BAD (enter the parameter name or its number).
bbn-simnet	Protocol Number 5208 (enter the parameter name or its number).
dec-mop-dump-ld	Protocol Number 6001 (enter the parameter name or its number).
dec-mop-rem-cdons	Protocol Number 6002 (enter the parameter name or its number).
dec-decnet	Protocol Number 6003 (enter the parameter name or its number).
dec-lat	Protocol Number 6004 (enter the parameter name or its number).
dec-diagnostic	Protocol Number 6005 (enter the parameter name or its number).
dec-customer	Protocol Number 6006 (enter the parameter name or its number).
dec-lavc	Protocol Number 6007 (enter the parameter name or its number).
rarp	Protocol Number 8035 (enter the parameter name or its number).
dec-lanbridge	Protocol Number 8038 (enter the parameter name or its number).
dec-encryption	Protocol Number 803D (enter the parameter name or its number).
appletalk	Protocol Number 809B (enter the parameter name or its number).

Parameter(cont.)	Description(cont.)
ibm-sna	Protocol Number 80D5 (enter the parameter name or its number).
appletalk-aarp	Protocol Number 80F3 (enter the parameter name or its number).
snmp	Protocol Number 814Cv.
ethertalk-2	Protocol Number 809B (enter the parameter name or its number).
ethertalk-2-aarp	Protocol Number 80F3 (enter the parameter name or its number).
ipx-snap	Protocol Number 8137 (enter the parameter name or its number).
ipx-802dot3	Protocol Number FFFF (enter the parameter name or its number).
ip	Protocol Number 0800 (enter the parameter name or its number).
ipx	Protocol Number 8137 (enter the parameter name or its number).
ipv6	Protocol Number 86DD (enter the parameter name or its number).

Mode Class Map Configuration

Examples To remove the eth-format and the protocol from the class-map `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match eth-format protocol
```

To set the eth-format to `ethii-tagged` and the protocol to `0800` (IP) for class-map `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match eth-format ethii-tagged protocol
0800
```

or

```
awplus(config-cmap)# match eth-format ethii-tagged protocol ip
```

match ip-precedence

Use this command to identify IP precedence values as match criteria.

Use the **no** variant of this command to remove IP precedence values from a class-map.

Syntax

```
match ip-precedence <0-7>
no match ip-precedence
```

Parameter	Description
<0-7>	The precedence value to be matched.

Mode Class Map Configuration

Example To configure a class-map named `cmap1` to evaluate all IPv4 packets for a precedence value of `5`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match ip-precedence 5
```

match mac-type

Use this command to set the MAC type for a class-map to match on.

Use **no** variant of this command to remove the MAC type match entry.

Syntax

```
match mac-type {l2bcast|l2mcast|l2ucast}
no match mac-type
```

Parameter	Description
l2bcast	Layer 2 Broadcast traffic.
l2mcast	Layer 2 Multicast traffic.
l2ucast	Layer 2 Unicast traffic.

Mode Class Map Configuration

Examples To set the class-map's MAC type to Layer 2 multicast, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match mac-type l2mcast
```

To remove the class-map's MAC type entry, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match mac-type
```

match tcp-flags

Sets one or more TCP flags (control bits) for a class-map to match on.

Use the **no** variant of this command to remove one or more TCP flags for a class-map to match on.

Syntax

```
match tcp-flags {[ack][fin][rst][syn][urg]}
no match tcp-flags {[ack][fin][rst][syn][urg]}
```

Parameter	Description
`ack`	Acknowledge.
`fin`	Finish.
`rst`	Reset.
`syn`	Synchronize.
`urg`	Urgent.

Mode Class Map Configuration

Examples To set the class-map's TCP flags to `ack` and `syn`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# match tcp-flags ack syn
```

To remove the TCP flags `ack` and `rst`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# no match tcp-flags ack rst
```

match vlan

Use this command to define the VLAN ID used as match criteria to classify a traffic class.

Use the **no** variant of this command to disable the VLAN ID used as match criteria.

Syntax

```
match vlan <1-4094>
no match vlan
```

Parameter	Description
<1-4094>	The VLAN number.

Mode Class Map Configuration

Examples To configure a class-map named `cmap1` to include traffic from VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match vlan
```

mls qos cos

This command assigns a CoS (Class of Service) user-priority value to untagged frames entering a specified interface. By default, all untagged frames are assigned a CoS value of 0.

Use the **no** variant of this command to return the interface to the default CoS setting for untagged frames entering the interface.

Syntax

```
mls qos cos <0-7>
no mls qos cos
```

Parameter	Description
<0-7>	The Class of Service, user-priority value.

Default By default, all untagged frames are assigned a CoS value of 0. Note that for tagged frames, the default behavior is not to alter the CoS value.

Mode Interface Configuration

Example To assign a CoS user priority value of 2 to all untagged packets entering ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# mls qos cos 2
```

mls qos enable

Use this command to globally enable QoS on the switch or stack.

Use the **no** variant of this command to globally disable QoS and remove all QoS configuration. The **no** variant of this command removes all class-maps, policy-maps, policers, and queue-sets that have been created. Running the **no mls qos** command will therefore remove all pre-existing QoS configurations on the switch.

Mode Global Configuration

Syntax

```
mls qos enable
no mls qos
```

Example To enable QoS on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos enable
```

mls qos map cos-queue to

Use this command to set the default CoS to egress queue mapping. This is the default queue mapping for packets that do not get assigned an egress queue via any other QoS functionality.

Use the **no** variant of this command to reset the cos-queue map back to its default setting. The default mappings for this command are:

```
CoS Priority :      0 1 2 3 4 5 6 7
--------------------------------
CoS QUEUE:          2 0 1 3 4 5 6 7
```

For more information see **"Mapping CoS tags to traffic types" on page 40.12**.

Syntax

```
mls qos map cos-queue <cos-priority> to <queue-number>
no mls qos map cos-queue
```

Parameter	Description
<cos-priority>	CoS priority value. Can take a value 0 to 7.
<queue-number>	Queue number. Can take a value 0 to 7.

Mode Global Configuration

Examples To set the cos-queue map back to its defaults, use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map cos-queue
```

To map CoS 2 to queue 0, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map cos-queue 2 to 0
```

Related Commands **show mls qos interface**

mls qos map premark-dscp to

This command configures the premark-dscp map. It is used when traffic is classified by a class-map that has **trust dscp** configured. Based on a lookup DSCP, the map determines a new DSCP, CoS, queue and bandwidth class for the traffic.

The **no** variant of this command resets the premark-dscp map to its defaults. If no DSCP is specified then all DSCP entries will be reset to their defaults.

Syntax

```
mls qos map premark-dscp <0-63> to {[new-dscp <0-63>][new-cos <0-7>]
    [new-bandwidth-class {green|yellow|red}]}

no mls qos map premark-dscp [<0-63>]
```

Parameter	Description
`premark-dscp <0-63>`	The DSCP value on ingress.
`new-dscp <0-63>`	The DSCP value that the packet will have on egress. If unspecified, this value will remain the DSCP ingress value.
`new-cos <0-7>`	The CoS value that the packet will have on egress. If unspecified, this value will retain its value on ingress.
`new-bandwidth-class`	Modify Egress Bandwidth-class. If unspecified, this value will be set to green.
`green`	Egress Bandwidth-class green (marked down Bandwidth-class).
`yellow`	Egress Bandwidth-class yellow (marked down Bandwidth-class).
`red`	Egress Bandwidth-class red (marked down Bandwidth-class).

Mode Global Configuration

Usage With the **trust dscp** command set, this command (**mls qos map premark-dscp**) enables you to make the following changes:

- remap the DSCP (leaving the other settings unchanged)
- remap any or all of CoS, output queue, or bandwidth class values (leaving the DSCP unchanged)

Note If you attempt to remap both the DSCP and another setting, only the DSCP remap will take effect.

Example 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 commands:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 1 to new-dscp 2
awplus(config)# mls qos map premark-dscp 2 to new-cos 3
awplus(config)# mls qos map premark-dscp 2 to new-queue 4
awplus(config)# mls qos map premark-dscp 2 to new-bandwidth-
class yellow
```

Example To set the entry for DSCP `1` to use a new DSCP of `2`, a new CoS of `3`, and a new bandwidth class of yellow, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 1 to new-dscp 2
new-cos 3 new-bandwidth-class yellow
```

Example To reset the entry for DSCP `1` use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map premark-dscp 1
```

Related Commands **show mls qos maps premark-dscp**
trust dscp

no police

Use this command to disable any policer previously configured on the class-map.

Syntax `no police`

Mode Policy Map Class Configuration

Usage This command disables any policer previously configured on the class-map.

Example To disable policing on a class-map use the command:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# no police
```

Related Commands police single-rate action
police twin-rate action

police single-rate action

Configures a single-rate policer for a class-map.

Syntax

```
police single-rate <cir> <cbs> <ebs> action {drop-red|
    remark-transmit}
```

Parameter	Description	
<cir>	Specify the Committed Information Rate (CIR) (1-16000000 kbps).	
<cbs>	Specify the Committed Burst Size (CBS) (0-16777216 bytes).	
<ebs>	Specify a Excess Burst Size (EBS) (0-16777216 bytes).	
`action`	Specify the action if the rate is exceeded.	
	`drop-red`	Drop the red packets.
	`remark-transmit`	Modify the packets using the *remark map*, then transmit. You can configure the remark map using the **remark-map** command on page 41.30.

Mode Policy Map Class Configuration

Usage You can use a policer to meter the traffic classified by the class-map and assign it to one of three bandwidth classes.

The bandwidth classes are green (conforming), yellow (partially-conforming), and red (non-conforming). A single-rate policer is based on three values. These are the average rate, minimum burst and maximum burst.

Color	Definition
`green`	The traffic rate is less than the average rate and minimum burst.
`yellow`	The traffic rate is between the minimum burst and the maximum burst.
`red`	The traffic rate exceeds the average rate and the maximum burst.

Using an action of drop-red means that any packets classed as red are discarded.

Note This command will not take effect when applied to a class-map that attaches to a channel group whose ports span processor instances.

Note that the **remark-map** does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green-colored and yellow-colored traffic irrespective of the value configured on the **action** parameter for the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to the fate of red-colored traffic. If **action** is set to **drop-red**, then red traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a single rate meter measuring traffic of 10 Mbps that drops a sustained burst of traffic over this rate, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police single-rate 10000 1875000 1875000
action drop-red
```

Related Commands
no police
police twin-rate action
remark-map

police twin-rate action

Configures a twin-rate policer for a class-map.

Syntax

```
police twin-rate <cir> <pir> <cbs> <pbs> action {drop-red|
    remark-transmit}
```

Parameter	Description	
`<cir>`	Specify the Committed Information Rate (CIR) (1-16000000 kbps).	
`<pir>`	Specify the Peak Information Rate (PIR) (kbps).	
`<pbs>`	Specify the Peak Burst Size (PBS) (0-16777216 bytes).	
`action`	Specify the action if rate is exceeded.	
	`drop-red`	Drop the red packets.
	`remark-transmit`	Modify the packets using the *remark map*, then transmit. You can configure the remark map using the **remark-map** command on page 41.30.

Mode Policy Map Class Configuration

Usage A policer can be used to meter the traffic classified by the class-map and as a result will be given one of three bandwidth classes. These are green (conforming), yellow (partially-conforming), and red (non-conforming).

A twin-rate policer is based on four values. These are the minimum rate, minimum burst size, maximum rate, and maximum burst size.

Bandwidth Class	Definition
`green`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is less than that set for the CBS.
`yellow`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is between those set for the CBS and the PBS.
`red`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time, result in a value that exceeds that set for the PBS.

Using an action of drop-red means that any packets classed as red will be discarded.

When using an action of remark-transmit the packet will be remarked with the values configured in the policed-dscp map. The index into this map is determined by the DSCP in the packet.

Note that the **remark-map** does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green-colored and yellow-colored traffic irrespective of the value configured on the **action** parameter fo the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to the fate of red-colored traffic. If **action** is set to **drop-red**, then red traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a twin rate meter measuring a minimum rate of 10 Mbps and a maximum rate of 20 Mbps that uses the premark map to remark any non-conforming traffic, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police twin-rate 10000 20000 1875000
3750000 action remark-transmit
```

Related Commands **no police**
police twin-rate action

policy-map

Use this command to create a policy-map and to enter Policy Map Configuration mode to configure the specified policy-map.

Use the **no** variant of this command to delete an existing policy-map.

Syntax

```
policy-map <name>
no policy-map <name>
```

Parameter	Description
<name>	Name of the policy-map.

Mode Global Configuration

Example To create a policy-map called `pmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#
```

Related Commands class-map

priority-queue

Configures strict priority based scheduling on the specified egress queues. You must specify at least one queue.

Syntax

```
priority-queue [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][1]...[7]`	Specify the queues that will use strict priority scheduling. With strict priority scheduling, the switch will completely empty the highest numbered queue first, then start processing the next lowest numbered queue.

Mode

Interface Configuration.

Usage

By default, the queues on all ports are set for priority queuing. You can change the queue emptying sequence to weighted round robin, by using the **wrr-queue weight queues** command on page 41.52. You can then use the **priority-queue** command to reset the selected queues to priority queuing.

Note that the emptying sequence for priority queuing is always highest queue number to lowest queue number.

Example

To apply priority based scheduling to egress queues 1 and 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# priority-queue 1 2
```

Related Commands

show mls qos interface
show mls qos interface queue-counters
wrr-queue weight queues

remark-map

Use this command to configure the remark map. If a re-mark map is applied to a class, and a policer is also applied to the same class, then:

- green and yellow traffic will *all* be acted upon by the remark-map, and
- red traffic will be either dropped or acted upon by the remark-map, depending on whether the policer **action** is set to **drop-red** or **remark-transmit**.

The **no** variant of this command resets the remark map to its defaults. Specifying the bandwidth class is optional. If no bandwidth class is specified, then all bandwidth classes are reset to their defaults.

Syntax

```
remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>]
    [new-bandwidth-class {green|yellow|red}]}

no remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp
    <0-63>] [new-bandwidth-class {green|yellow|red}]}
```

Parameter	Description
`bandwidth-class`	Specify the bandwidth class of packets to remark.
`green`	Remark green packets.
`yellow`	Remark yellow packets.
`red`	Remark red packets.
`new-dscp`	Specify the new DSCP value.
<0-63>	The DSCP value.
`new-bandwidth-class`	Specify the new bandwidth class.
`green`	Remark the packet green.
`yellow`	Remark the packet yellow.
`red`	Remark the packet red.

Mode Policy Map Class Configuration

Examples To remark the policed green traffic to a new DSCP of `2` and a new bandwidth class of `yellow`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to
new-dscp 2 new-bandwidth-class yellow
```

To remark the policed green traffic to a new DSCP of 2, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to
new-dscp 2
```

To reset the DSCP for all bandwidth classes, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no remark-map to new-dscp
```

Related Commands **police single-rate action**
police twin-rate action

remark new-cos

This command enables you to configure and remark either or both of:

- the CoS flag in the data packet
- the input into the CoS to queue map, thus changing the destination egress queue.

Syntax

```
remark new-cos <0-7> [internal|external|both]
no remark new-cos [internal|external|both]
```

Parameter	Description
<0-7>	The new value for the CoS flag and/or the input into the CoS to queue map.
`external`	Remarks the CoS flag in the packet.
`internal`	Remarks the new-CoS input into the CoS to queue map.
`both`	Remarks (with the same value) both the CoS flag in the packet and the input to the CoS to queue map.

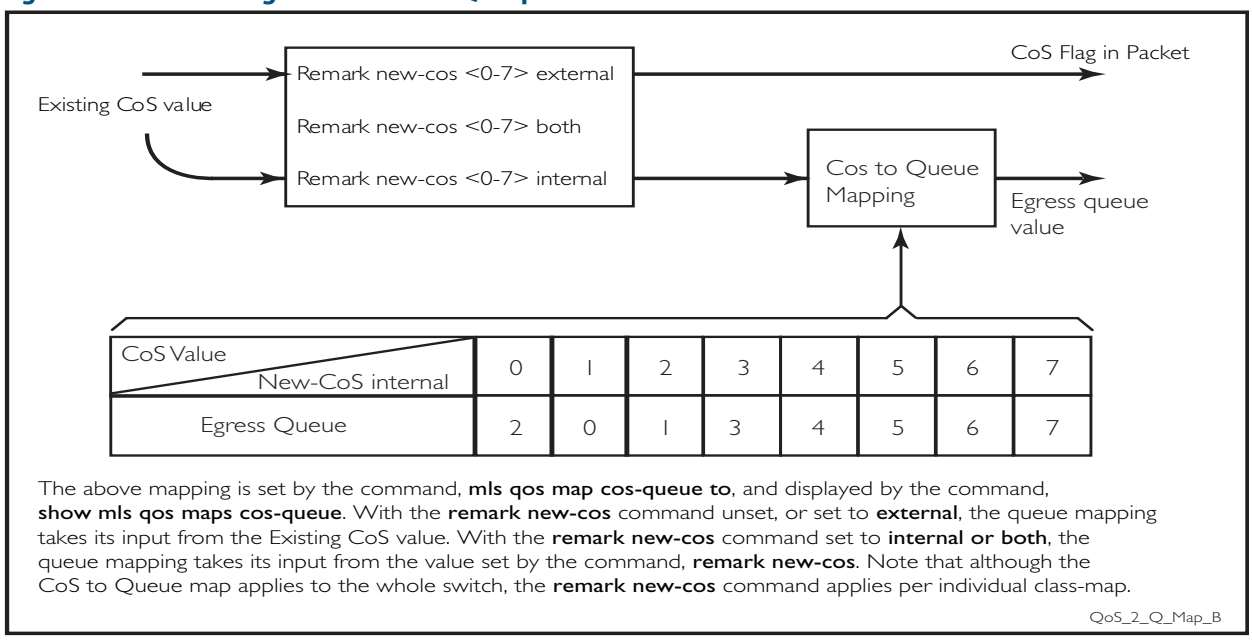
Mode Policy Map Class Configuration

Usage The default CoS to Queue mappings are shown in the following table:

CoS Value	0	1	2	3	4	5	6	7
Egress Queue No	2	0	1	3	4	5	6	7

The relationship between this command and the CoS to queue map is shown in **Figure 41-1**.

Figure 41-1: Remarking and the CoS to Q map



The above mapping is set by the command, **mls qos map cos-queue to**, and displayed by the command, **show mls qos maps cos-queue**. With the **remark new-cos** command unset, or set to **external**, the queue mapping takes its input from the Existing CoS value. With the **remark new-cos** command set to **internal or both**, the queue mapping takes its input from the value set by the command, **remark new-cos**. Note that although the CoS to Queue map applies to the whole switch, the **remark new-cos** command applies per individual class-map.

QoS_2_Q_Map_B

Table 41-1: CoS to egress queue remarking function

Input	Command	Output
CoS field = 1	Remark new-cos (not configured)	CoS value = 1 Packet sent to egress queue 0
CoS field = 1	Remark new-cos 2 external	CoS value = 2 Packet sent to egress queue 0
CoS set to 1	Remark new-cos 2 internal	CoS value = 1 Packet sent to egress queue 1
CoS set to 1	Remark new-cos 2 both	CoS value = 2 Packet sent to egress queue 1
Note: This table assumes that the CoS to Queue map is set to its default values.		

Example For policy-map `pmap3` and class-map `cmap1`, set the CoS value to `2` and also set the input to the CoS to queue map so that the traffic is assigned to egress queue 1:

```
awplus# configure terminal
awplus(config)# policy-map pmap3
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark new-cos 2 both
```

Related Commands **mls qos map cos-queue to**
show mls qos maps cos-queue

service-policy input

Use this command to apply a policy-map to the input of an interface.

Use the **no** variant of this command to remove a policy-map and interface association.

Syntax

```
service-policy input <policy-map>
no service-policy input <policy-map>
```

Parameter	Description
<policy-map>	Policy map name that the input will applied to.

Mode Interface Configuration

Usage This command can be applied to switch ports or static channel groups, but not to dynamic (LACP) channel groups.

Example To apply a policy-map named `pmap1` to interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# service-policy input pmap1
```

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
<class-map name>	Name of the class-map.

Mode User Exec and Privileged Exec

Example To display the QoS class-maps to define the match criteria to classify traffic, use the command:

```
awplus# show class-map cmap1
```

Output **Figure 41-2: Example output from the show class-map command**

```
CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
```

Related Commands class-map

show mls qos

Use this command to display whether QoS is enabled or disabled on the switch.

Syntax `show mls qos`

Mode User Exec and Privileged Exec

Example To display whether QoS is enabled or disabled, use the command:

```
awplus# show mls qos
```

Output **Figure 41-3: Example output from the show mls qos command**

```
awplus#show mls qos
 Enable
```

Related Commands mls qos enable

show mls qos interface

Displays the current settings for the interface. This includes its default CoS and queue, scheduling used for each queue, and any policies/maps that are attached.

Syntax `show mls qos interface [<port>]`

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To display current CoS and queue settings for interface `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1
```

Output **Figure 41-4: Example output from the show mls qos interface command**

```
Default CoS:   7
    Default Queue: 7
    Number of egress queues: 8
    Queue Set: 1
    Egress Queue:         0
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         1
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         2
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         3
      Status:             Enabled
      Scheduler:          Wrr Group 2
      Weight:             10
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         4
      Status:             Enabled
      Scheduler:          Wrr Group 1
      Weight:             10
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         5
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         6
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
    Egress Queue:         7
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
```

Table 41-2: Parameters in the output of the show mls qos interface command

Parameter	Description
`Default CoS`	The default CoS priority that will be applied to all packets arriving on this interface.
`Default Queue`	The default queue that will be applied to all packets arriving on this interface.
`Number of egress queues`	The total number of egress queues available on this interface.
`Queue Set`	Drop queue set that has been applied to the port. This could either be operating in threshold or random-detect mode.
`Egress Queue X`	Number of this egress queue.
`Status`	Queue can either be enabled or disabled.
`Scheduler`	The scheduling mode being used for servicing the transmission of packets on this port.
`Queue Limit`	The percentage of the port's buffers that have been allocated to this queue.
`Egress Rate Limit`	The amount of traffic that can be transmitted via this queue per second. 0 Kb means there is currently no rate-limiting enabled.

show mls qos interface policer-counters

This command displays an interface's policer counters. This can either be for a specific class-map or for all class-maps attached to the interface. If no class-map is specified then all class-map policer counters attached to the interface are displayed.

Note that these counters are based on metering performed on the specified class-map. Therefore, the '`Dropped Bytes`' counter is the number of bytes dropped due to metering. This is different from packets dropped via a 'deny' action in the ACL. If a policer is configured to perform re-marking, bytes can be marked Red but are not dropped, and is shown with a value of 0 for the Dropped field and a non-0 value for the '`Red Bytes`' field.

Syntax

```
show mls qos interface <port> policer-counters
   [class-map <class-map>]
```

Parameter	Description
<port>	Switch port.
`class-map`	Select a class-map.
<class-map>	Class-map name.

Mode User Exec and Privileged Exec

Usage Note that the hardware does not record distinct counters for the number of Green or Yellow bytes, so the field marked Green/Yellow is the summation of bytes that have been marked Green or Yellow by the meter.

Example To show the counters for all class-maps attached to `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1 policer-counters
```

Output **Figure 41-5: Example output from show mls qos interface policer-counters**

```
awplus#show mls qos int port1.0.1 policer-counters
Interface:               port1.0.1
  Class-map:             default
    Green/Yellow Bytes:  0
    Red Bytes:           0
    Dropped Bytes:       0
    Non-dropped Bytes:   0
  Class-map:             cmap1
    Green/Yellow Bytes:  1629056
    Red Bytes:           7003200
    Dropped Bytes:       0
    Non-dropped Bytes:   8632256
```

This output shows a policer configured with remarking through '`action remark-transmit`', so although bytes are marked as Red, none are dropped. Therefore, the '`Non-dropped Bytes`' field shows a summation of Green/Yellow and Red bytes.

show mls qos interface queue-counters

This command displays an interface's egress queue counters. This can either be for a specific queue or for all queues on the interface. If no queue is specified all queue counters on the interface will be displayed.

The counters show the number of frames currently in the queue and the maximum number of frames allowed in the queue, for individual egress queues and the port's queue (which will be a sum of all egress queues).

Syntax `show mls qos interface <port> queue-counters [queue <0-7>]`

Parameter	Description
<port>	Switch port.
<0-7>	Queue.

Mode User Exec and Privileged Exec

Example To show the counters for all queues on `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1 queue-counters
```

Output **Figure 41-6: Example output from the show mls qos interface queue-counters command**

```
Interface port1.0.4 Queue Counters:
  Port queue length     1169
  Egress Queue length:
    Queue 0                0
    Queue 1                0
    Queue 2             1169
    Queue 3                0
    Queue 4                0
    Queue 5                0
    Queue 6                0
    Queue 7                0
```

Table 41-3: Parameters in the output of the show mls qos interface queue-counters command

Parameter	Description
`Interface`	Port we are showing the counters for.
`Port queue length`	Number of frames in the port's queue. This will be the sum of all egress queues on the port.
`Egress Queue length`	Number of frames in a specific egress queue.

show mls qos interface storm-status

Show the current configuration and status of the QoS Storm Protection (QSP) on the given port.

Syntax `show mls qos interface <port> storm-status`

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To see the QSP status on `port1.0.1`, use command:

```
awplus# show mls qos interface port1.0.1 storm-status
```

Output **Figure 41-7: Example output from the show mls qos interface storm-status command**

```
Interface:           port1.0.1
Storm-Protection:    Enabled
Port-status:         Enabled
Storm Action:        vlandisable
Storm Window:        5000 ms
Storm Downtime:      0 s
Timeout Remaining:   0 s
Last read data-rate: 0 kbps
Storm Rate:          1000 kbps
```

Related Commands
storm-action
storm-downtime
storm-protection
storm-rate
storm-window

show mls qos maps cos-queue

Show the current configuration of the cos-queue map.

Syntax `show mls qos maps cos-queue`

Mode User Exec and Privileged Exec

Example To display the current configuration of the cos-queue map, use the command:

```
awplus# show mls qos maps cos-queue
```

Output **Figure 41-8: Example output from the show mls qos maps cos-queue command**

```
COS-TO-QUEUE-MAP:
      COS :           0 1 2 3 4 5 6 7
      --------------------------------
      QUEUE:          0 7 1 3 4 5 6 7
```

Related Commands mls qos map cos-queue to

show mls qos maps premark-dscp

This command displays the premark-dscp map. This map is used when the **trust dscp** command has been specified for a policy-map's class-map to replace the DSCP, CoS, queue, and bandwidth class of a packet matching the class-map based on a lookup DSCP value.

Syntax `show mls qos maps premark-dscp [<0-63>]`

Parameter	Description
<0-63>	DSCP table entry.

Mode User Exec and Privileged Exec

Example To display the premark-dscp map for DSCP `1`, use the command:

```
awplus# show mls qos maps premark-dscp 1
```

Output **Figure 41-9: Example output from the show mls qos maps premark-dscp command**

```
PREMARK-DSCP-MAP:

    DSCP 1
    Bandwidth Class         Green    Yellow   Red
    ------------------------------------------------
    New DSCP                1        -        -
    New CoS                 0        -        -
    New Queue               0        -        -
    New Bandwidth Class     green    -        -
```

Related Commands **mls qos map premark-dscp to**
trust dscp

show policy-map

Displays the policy-maps configured on the switch. The output also shows whether or not they are connected to a port (attached / detached) and shows their associated class-maps.

Syntax `show policy-map [<name>]`

Parameter	Description
<name>	The name of a specific policy-map.

Mode User Exec and Privileged Exec

Example To display a listing of the policy-maps configured on the switch, use the command:

```
awplus# show policy-map
```

Output **Figure 41-10: Example output from the show policy-map command**

```
POLICY-MAP-NAME: general-traffic
  State: attached
    Default class-map action: permit
    CLASS-MAP-NAME: default
    CLASS-MAP-NAME: database-traffic
```

Related Commands service-policy input

storm-action

Sets the action to take when triggered by QoS Storm Protection (QSP). There are three available options:

- **portdisable** will disable the port in software.
- **vlandisable** will disable the port from the VLAN matched by the class-map in class-map.
- **linkdown** will physically bring the port down. The **vlandisable** requires the match vlan class-map to be present in the class-map.

The **no** variant of this command will negate the action set by the **storm-action** command.

Syntax

```
storm-action {portdisable|vlandisable|linkdown}
no storm-action
```

Parameter	Description
`portdisable`	Disable the port in software.
`vlandisable`	Disable the VLAN.
`linkdown`	Shutdown the port physically.

Mode Policy Map Class Configuration

Examples To apply the storm protection of `vlandisable` to the policy-map named `pmap2`, and the class-map named `cmap1`, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# storm-action vlandisable
```

To negate the storm protection set on the policy-map named `pmap2`, and the class-map named `cmap1`, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# no storm-action
```

Related Commands
storm-downtime
storm-protection
storm-rate
storm-window

storm-downtime

Sets the time to re-enable the port once disabled by QoS Storm Protection (QSP). The time is given in seconds, from a minimum of one second to maximum of 86400 seconds (i.e. one day).

The **no** variant of this command resets the time to the default value of 10 seconds.

Syntax

```
storm-downtime <1-86400>
no storm-downtime
```

Parameter	Description
<1-86400>	Seconds.

Default 10 seconds

Mode Policy Map Class Configuration

Examples To re-enable the port in 1 minute, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# storm-downtime 60
```

To re-set the port to the default (10 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no storm-downtime
```

Related Commands

storm-action
storm-protection
storm-rate
storm-window

storm-protection

Use this command to enable the Policy Based Storm Protection (such as QSP - QoS Storm Protection). Storm protection is activated as soon as a port is enabled.

The **no** variant of this command disables Policy Based Storm Protection.

Syntax

```
storm-protection
no storm-protection
```

Default By default, storm protection is disabled.

Mode Policy Map Class Configuration

Examples To enable QSP on `cmap2` in `pmap2`, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-protection
```

To disable QSP on `cmap2` in `pmap2`, use the following commands:

```
awplus# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-protection
```

Related Commands

storm-action
storm-downtime
storm-rate
storm-window

storm-rate

Sets the data rate that triggers the storm-action. The rate is in kbps and the range is from 1kbps to 10Gbps.

Note that this setting is made in conjunction with the **storm window** command.

Use the **no** variant of this command to negate the **storm-rate** command.

Syntax

```
storm-rate <1-10000000>
no storm-rate
```

Parameter	Description
<1-10000000>	The range of the storm-rate.

Default No default

Mode Policy Map Class Configuration

Usage This setting is made in conjunction with the **storm-window** command on page 41.49.

Examples To the limit to 1Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-rate 1000
```

To negate the limit set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-rate 1000
```

Related Commands

storm-action
storm-downtime
storm-protection
storm-window

storm-window

Sets the window size of QoS Storm Protection (QSP). This sets the time to poll the data-rate every given milliseconds. Minimum window size of 100 ms and the maximum is 60 sec.

Use the **no** variant of this command to negate the **storm-window** command.

Syntax

```
storm-window <100-60000>
no storm-window
```

Parameter	Description
<100-60000>	The window size, measured in milliseconds.

Default No default

Mode Policy Map Class Configuration

Usage This command should be set in conjunction with the **storm-rate** command on page 41.48.

Examples To set the QSP window size to `5000` ms, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-window 5000
```

To negate the QSP window size set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-window 5000
```

Related Commands

storm-action
storm-downtime
storm-protection
storm-rate

trust dscp

This command enables the premark-dscp map to replace the bandwidth-class, CoS, DSCP, and queue of classified traffic based on a lookup DSCP value.

With the no variant of this command, no premark-dscp mapping function will be applied for the selected class-map. QoS components of the packet existing either at ingress, or applied by the class-map, will pass unchanged.

Syntax

```
trust dscp
no trust
```

Mode Policy-Map Configuration. Because policy-maps are applied to ports, you can think of **trust dscp** as a per-port setting.

Examples To enable the premark-dscp map lookup for policy-map `pmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# trust dscp
```

To disable the premark-dscp map lookup for policy-map `pmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no trust
```

Related Commands mls qos map premark-dscp to

wrr-queue disable queues

Use this command to disable an egress queue from transmitting traffic.

The **no** variant of this command enables an egress queue to transmit traffic.

Syntax

```
wrr-queue disable queues [0][1][2][3][4][5][6][7]
no wrr-queue disable queues [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][2]...[7]`	Selects one or more queues numbered 0 to 7.

Mode Interface Configuration

Examples To enable queue 1 to transmit traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no wrr-queue disable queues 1
```

To disable queue 1 from transmitting traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue disable queues 1
```

Related Commands **show mls qos interface**

wrr-queue weight queues

This command configures weighted round-robin based scheduling on the specified egress queues on switch port interfaces only. The weights are specified as ratios relative to each other. It does not matter which numbers you use, only their ratio.

Syntax `wrr-queue weight <1-15> queues [0][1][2][3][4][5][6][7]`

Parameter	Description
`<1-15>`	Weight (the higher the number the greater will be the queue servicing).
`[0][1]...[7]`	Enter egress queue numbers 0-7, to assign the specified queues the specified weight.

Mode Interface Configuration for switch port interfaces only (not for static aggregated interfaces).

Usage Only apply weighted round-robin based scheduling to switch port interfaces (for example, `awplus(config)#interface port1.0.2`).

You cannot apply weighted round-robin based scheduling to static aggregated interfaces (for example, `awplus(config)#interface sa2`). Attempting to apply weighted round-robin based scheduling on aggregated interfaces will display the console error shown below:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# wrr-queue weight
% Invalid input detected at ^ marker
```

Example To apply a WRR weight of `6` to queues 0 and 1 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue weight 6 queues 0 1
```

Related Commands **priority-queue**
show mls qos interface

Chapter 42: Authentication Introduction and Configuration

Authentication Introduction 42.2
Configuring a Guest VLAN 42.2
802.1X-Authentication 42.3
Web-Authentication 42.4
What is Web-Authentication? 42.4
Web-Authentication Basics 42.4
Configuring Web-Authentication 42.6
Starting a Web-Authentication Session 42.8
Configuring an External Login Page 42.10
Customizing Web-Authentication Login Page 42.13
Support for Protocols Underlying Web-Authentication 42.15
Web-Authentication Timeout Connect 42.20
Web Authorization Proxy 42.21
MAC-Authentication 42.22
Why is MAC-Authentication Required? 42.22
How Does MAC-Authentication Work? 42.22
Configuring MAC-Authentication 42.23
Tri-Authentication 42.24
Tri-Authentication Configuration 42.25
Two-Step Authentication 42.27
Ensuring Authentication Methods Require Different Usernames and Passwords 42.28
Roaming Authentication 42.29
Roaming Authentication Overview 42.30
Roaming Authentication Feature Interactions 42.31
Unauthenticated Supplicant Traffic 42.32
Deciding When a Supplicant Fails Authentication 42.34
Failed Authentication VLAN 42.35
Limitations on Allowed Feature Combinations 42.35

Authentication Introduction

Authentication commands enable you to specify three different types of device authentication: 802.1X-Authentication, Web-Authentication, and MAC-Authentication.

802.1X is an IEEE standard providing a mechanism for authenticating devices attached to a LAN port or wireless device. Web-Authentication is applicable to devices that have a human user who opens the web browser and types in a user name and password when requested. MAC-Authentication is used to authenticate devices that have neither a human user nor implement 802.1X supplicant when making a network connection request.

Configuring a Guest VLAN

In a secure network, the default behavior is to deny any access to supplicants that cannot be authenticated. However, it is often convenient to allow unauthenticated users to have limited access. A popular solution is to define a limited-access VLAN, called the Guest VLAN, and assign unauthenticated users into that VLAN. Unauthenticated supplicants are either supplicants who have attempted and failed authentication or haven't performed any authentication.

See the **auth guest-vlan** command on page 43.9 for command information about Guest VLAN.

By default, traffic from unauthenticated supplicants in the Guest VLAN will only be L2 switched within the Guest VLAN. But, if the **routing** parameter for the **auth guest vlan** command is configured, then the switch will route unauthenticated supplicants' traffic to other VLANs if required, and will relay their DHCP requests to servers in other VLANs if required.

You can configure 802.1X to accept a Dynamic VLAN assignment, or fall back to a Guest VLAN upon failure.

To configure a switch to perform 802.1X-Authentication, and assign VLAN IDs to ports where devices authentication successfully, and put non-authenticated users into a Guest VLAN, proceed as follows:

```
awplus# configure terminal
awplus(config)# radius-server host <ip-address> key
<key-string>
awplus(config)# aaa authentication dot1x default group
radius
awplus(config)# interface <interface-range>
awplus(config-if)# switchport mode access
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth guest-vlan 100
```

802.1X-Authentication

802.1X is an IEEE standard providing a mechanism for authenticating devices attached to a LAN port or wireless device. Devices wishing to access services behind a port must authenticate themselves before any Ethernet packets are allowed to pass through. The protocol is referred to as 802.1X because it was initially defined in the IEEE standard 802.1X, published in 2001 and revised in 2004 and again as the current 802.1X 2010 standard.

For more information about 802.1X, see **Chapter 46, 802.1X Introduction and Configuration**.

Web-Authentication

What is Web-Authentication?

Web-Authentication is a convenient alternative to 802.1X-Authentication. It's commonly used to authenticate users in educational institutions, where regular users' workstations are not managed by the network administrator. Web-Authentication enables the switch to detect an unauthenticated workstation web browsing into the network, then redirect the user's web browser to its own authentication web page.

Web-Authentication works like this:

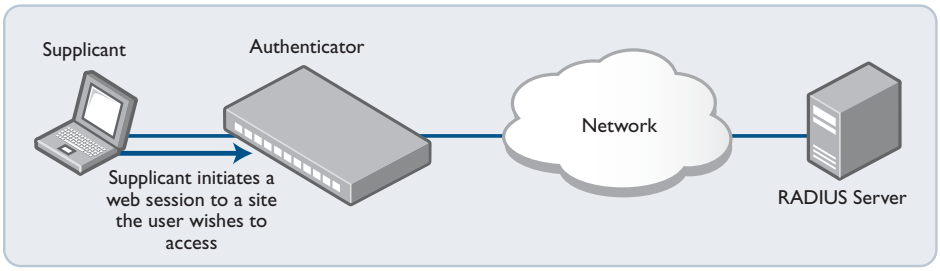
- The user enters their username and password into the web page, which the switch then sends to a RADIUS server for checking.
- If the RADIUS server accepts the user's credentials, the switch then allows their traffic into the network.

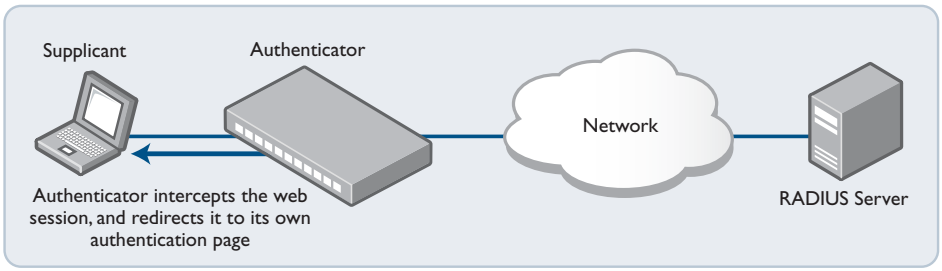
The Web-authenticating switch interacts with a RADIUS server in the same way as an 802.1X authenticator. The two methods can be used together in the same network, using the same RADIUS server.

Web-Authentication Basics

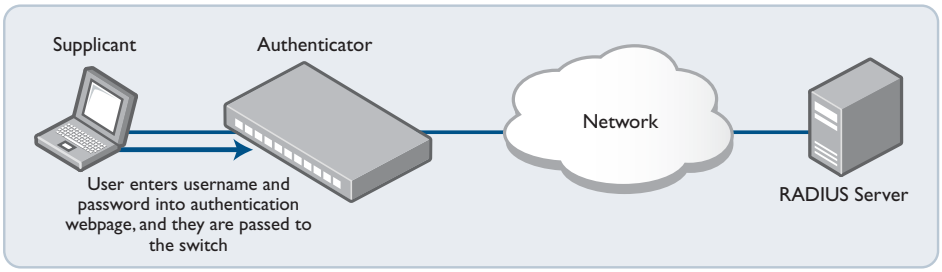
The operation of Web-Authentication is explained as below:

1. The authenticating switch receives HTTP or HTTPS traffic from an unauthenticated supplicant. It intercepts the supplicant's web session and redirects it to its own internal web server.

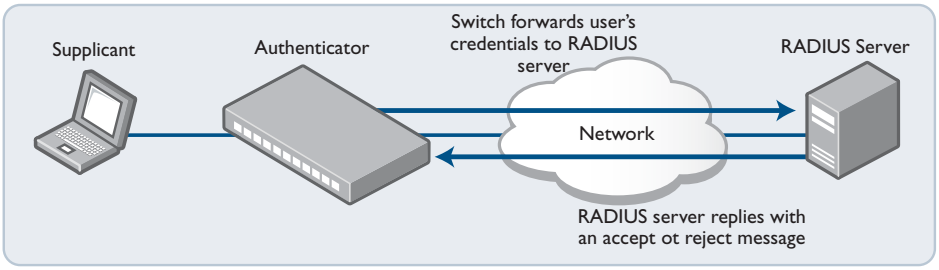




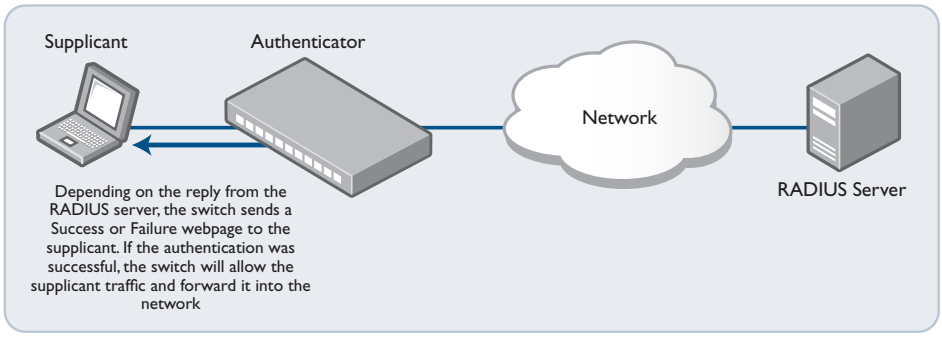
2. The web server serves up an authentication page on which the user enters their username and password.



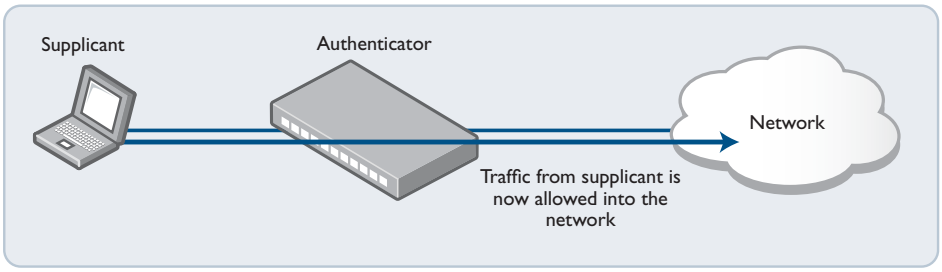
3. The username and password are sent to a RADIUS server, which informs the authenticating switch whether or not the supplicant is authenticated.



4. The user is then informed of the RADIUS server's verdict.



5. If the supplicant has been successfully authenticated, the authenticating switch will give the supplicant workstation access to the network.



Configuring Web-Authentication

Web-Authentication can be configured on a switch in the following steps:

1. Configure a RADIUS server.

```
awplus(config)# radius-server host <server-ip-address> key
                <shared-secret>
```

2. Instruct Web-Authentication to use the configured RADIUS server.

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

3. Define the IP address through which the Web-Authentication service will be accessed.

```
awplus(config)# auth-web-server ipaddress <ip-address>
```

4. Configure ports for Web-Authentication.

```
        awplus# interface port1.0.1-1.0.6
awplus(config)# auth-web enable
```

Choosing the Web-Authentication server address

When you come to configure Web-Authentication, you need to answer some questions:

Questions What IP address should I specify as the Web-Authentication server address? Is it okay to use just any IP address that is configured on one of the switch's VLANs, or is the choice more constrained than that?

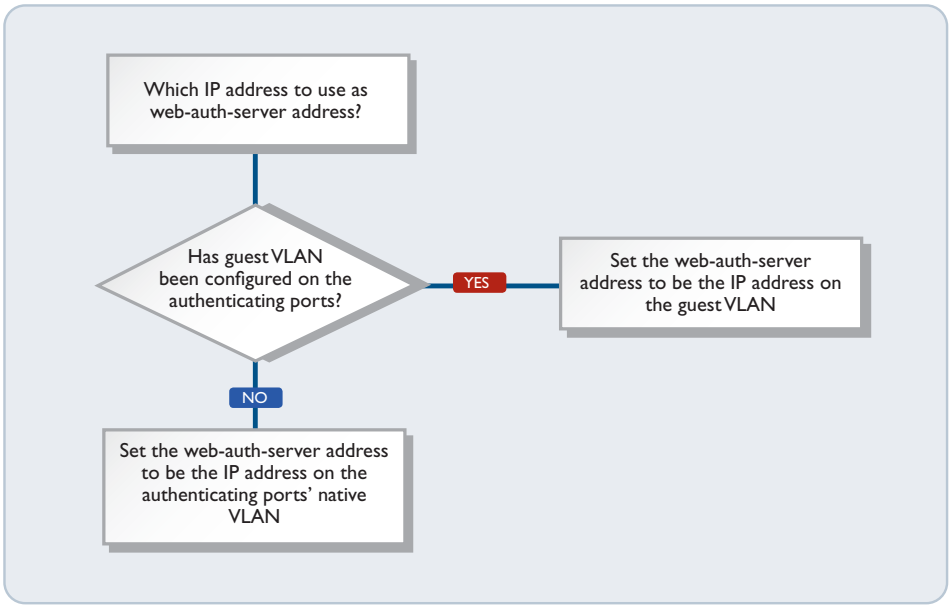
Answer You must use the IP address that is configured on the VLAN that the supplicant's packets will arrive on.

The logic that the switch uses in deciding which VLAN to associate non-authenticated supplicants' packets with is:

- If guest VLAN has been configured on the port where the packet arrives, then associate the packet with the guest VLAN.
- Otherwise associate the packet with the port's native VLAN.

If you configure the supplicant-connected ports with guest VLAN, then use the IP address on the guest VLAN as the IP address of the Web-Authentication server. Otherwise use the IP address on the supplicant-connected ports' native VLAN.

The diagram below illustrates how to decide which IP address to use as the Web-auth-server address:



Configuration Example 1: Using a guest VLAN

```
VLAN database
    VLAN 20 name guest
    VLAN 10 name edge
    VLAN 30 name core

radius-server host 192.168.30.129 key verysecret
aaa authentication auth-Web default group RADIUS
auth-Web-server ipaddress 192.168.20.1

int vlan10
    ip address 192.168.10.1/24
int vlan20
    ip address 192.168.20.1/24
int vlan30
ip address 192.168.30.1/24

int port1.0.1-1.0.3
  switchport access vlan 10
 auth-Web enable
  auth guest-vlan 20

int port1.0.4-1.0.6
  switchport access vlan 30
```

Configuration Example 2: Not using a guest VLAN

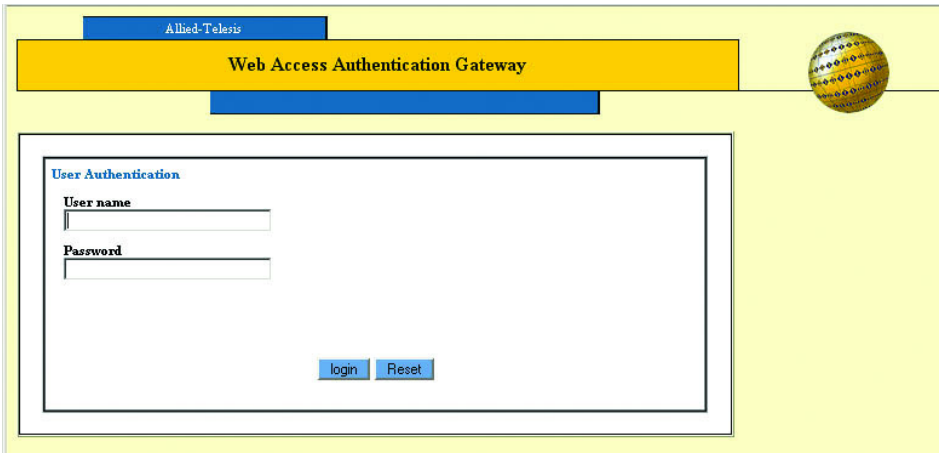
```
VLAN database
    VLAN 10 name edge
    VLAN 30 name core

radius-server host 192.168.30.129 key verysecret
aaa authentication auth-web default group radius
auth-web-server ipaddress 192.168.10.1

int vlan10
    ip address 192.168.10.1/24
int vlan30
ip address 192.168.30.1/24

int port1.0.1-1.0.3
  switchport access vlan 10
  auth-Web enable

int port1.0.4-1.0.6
  switchport access vlan 30
```

Starting a Web-Authentication Session

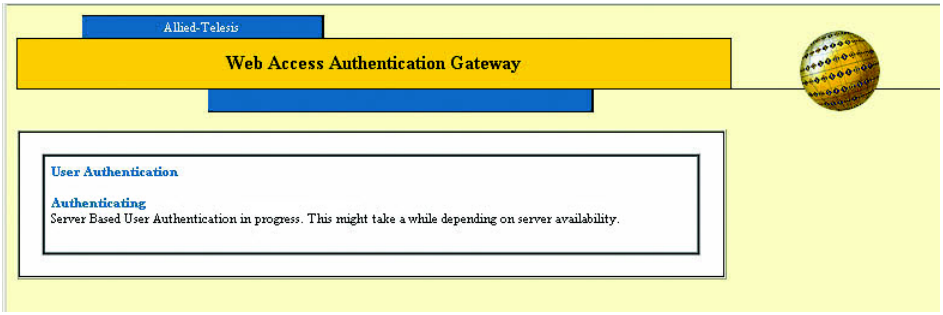
This section explains what the user actually sees in a Web-Authentication session:

1. The user starts their Web browser, and browses to a page they wish to view. Shortly thereafter, the address in the browser's address bar automatically changes to the address of the authenticating switch's authentication page.

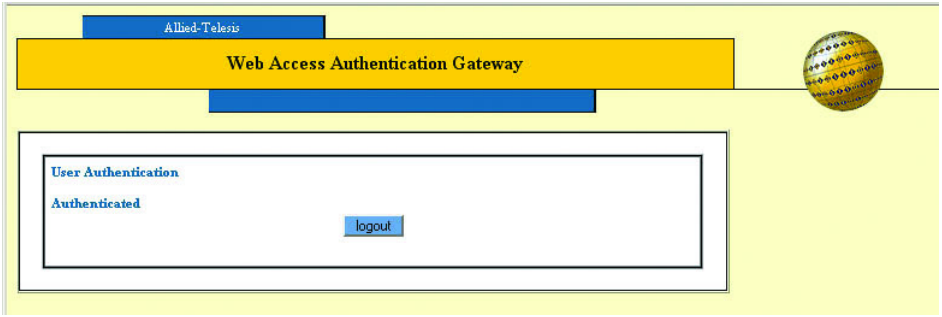
2. In the switch's authentication page, the user enters their user name and password, and clicks **login**. The maximum length of the user name and password is 64 characters. The local RADIUS server has a password length limit of 31 characters.



3. The switch displays a page that informs them that authentication is in progress.

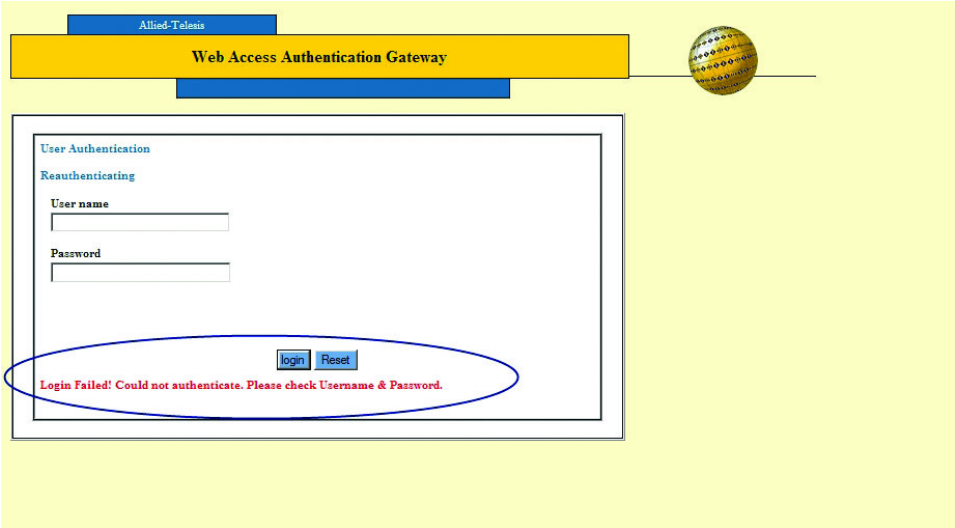


4. Once authentication is complete, the authentication result is displayed.



If the user enters a username/password combination that is not accepted by the RADIUS server, the switch presents an invitation to check the username and password.

If the user enters incorrect usernames/passwords several times, the authentication fails. The number of times a user can try to login is configurable but it is set to 10 by default.

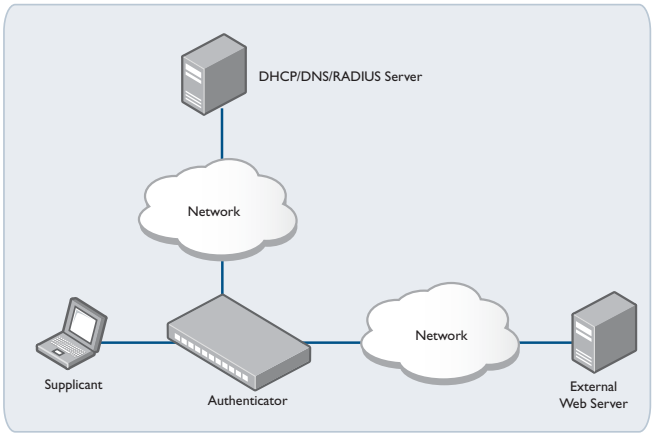


Configuring an External Login Page

This section explains how to configure an external login page for Web-Authentication rather than using the built-in AlliedWare Plus login page.

In this configuration example, a remote DHCP server is used to allocate IP addresses to the supplicants. You can also configure Authenticator as a local DHCP server.

Note that routing in the network must be set up so that packets can be routed directly between the supplicant and the external web server.



1. Configure the IP address for vlan1 to be used to reach remote DHCP/DNS/RADIUS server.

```
awplus(config)# int vlan1
awplus(config-if)# ip address 192.168.1.2/24
```

2. Configure the remote DNS server on Authenticator.

```
awplus(config)# ip name-server x.x.x.x
awplus(config)# ip dns forwarding
```

3. Configure auth-web on Authenticator

```
awplus(config)# aaa authentication auth-web default group
                radius
awplus(config)# int port1.0.1
awplus(config-if)# auth-web enable
```

4. Configure the remote RADIUS server on Authenticator. You can also configure Authenticator as a local RADIUS server.

```
awplus(config)# radius-server host 192.168.1.254 key 123
```

5. Configure the external login page by using the **auth-web-server login-url** command. You can use the domain name or the IP address for the external web server. In this example, the IP address of the external web server is 192.168.1.1. You also need to allow HTTP packets to the external login server to be forwarded by using the **auth-web forward** command. If the external web server is using another TCP port other than 80, you need to change 80 to the corresponding port number.

```
awplus(config)# auth-web-server login-url http://
                192.168.1.1/login.html
awplus(config-if)# auth-web forward 192.168.1.1 tcp 80
```

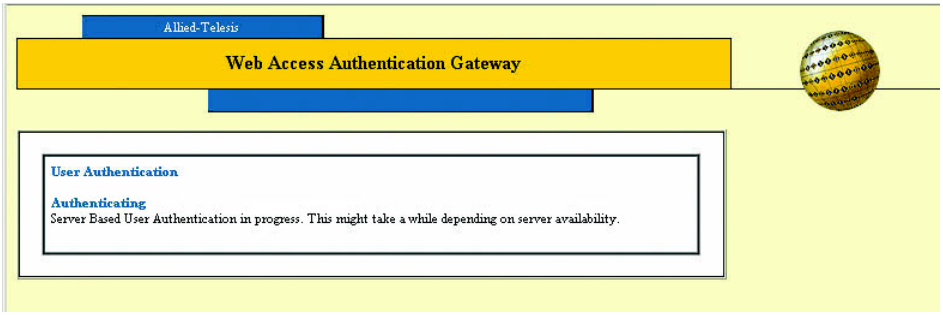
Supplicant Login

This section explains what the user actually sees in an external Web-Authentication session.

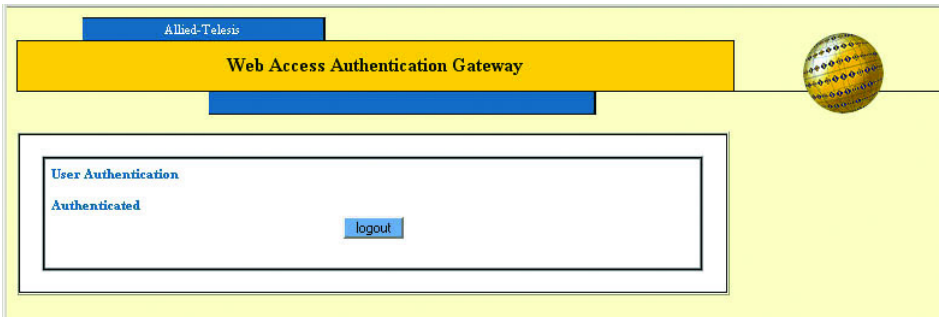
1. When a supplicant tries to access any website, the supplicant will be redirected to the external login page for authentication.

2. On the device's authentication page, the user enters their user name and password, and clicks **login**.

3. The device displays a page that informs them that authentication is in progress.



4. Once authentication is complete, the authentication result is displayed.



If the user enters a username/password combination that is not accepted by the RADIUS server, the device presents an invitation to check the username and password.

External Supplicant Login Page Support

A file named login.html must be present on the external web server. The file must contain the following elements:

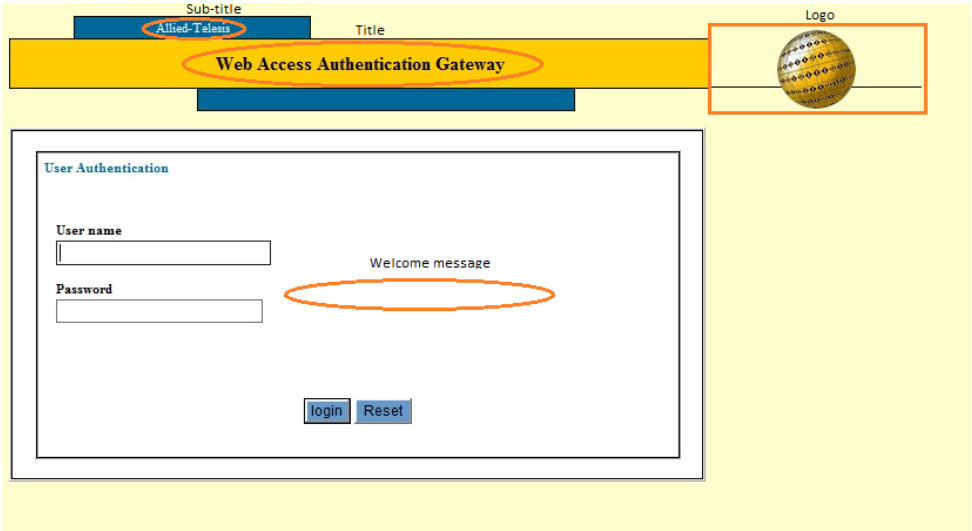
```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8" />
    <title>HTML 5 complete</title>
  </head>
  <body>
    <form action="http://<Authenticator IP address>/index.cgi"
autocomplete="off" target="_self" name="AUTH" method="POST">
      <div>User name</div>
      <div><input size="30" type="text" maxlength="64"
name="USERNAME"></div>
      <div>Password</div>
      <div><input size="30" type="password" maxlength="64"
name="PASSWORD"></div>
      <div>
        <input type="submit" name="ACTION" value="login">
        <input type="reset" name="RESET" value="Reset">
      </div>
    </form>
  <body>
</html>
```

Note that Authenticator and the external web server don't communicate with each other. The role of the external web server is just to serve a custom login page.

Also note that the external login server feature and the auth-web dhcp server feature are mutually exclusive. You cannot configure auth-web-server login-url and auth-web-server dhcp ipaddress at the same time.

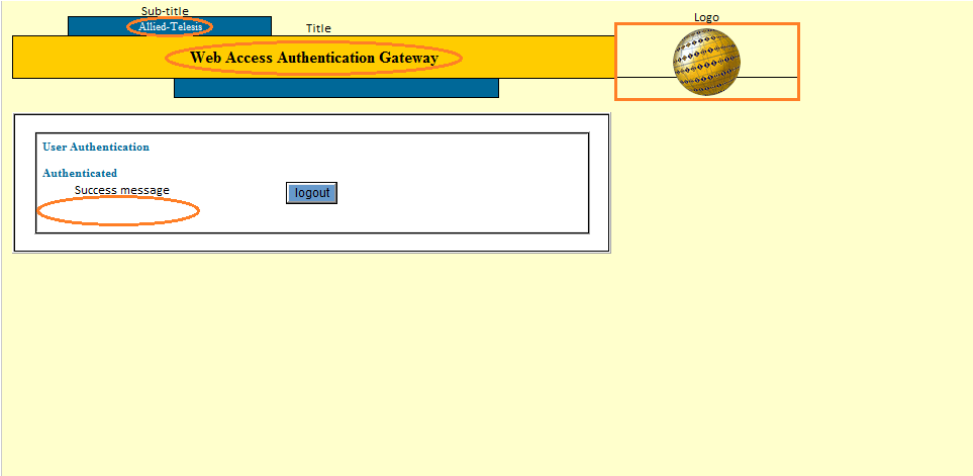
Customizing Web-Authentication Login Page

You can customize the Web-Authentication page by changing the web page logo image, success message, welcome message, web page title and sub-title. For more information



about the commands used to customize the page, see **Chapter 43, Authentication**

Commands. The elements that can be customized are shown below:



- To set the custom sub-title and title on the Web-Authentication page, use the commands below:

```
auth-web-server page sub-title {hidden|text <sub-title>}
auth-web-server page title {hidden|text <title>}
```

- To set the success and welcome message appearing on the Web-Authentication page, use the commands below:

```
auth-web-server page welcome-message text <welcome-message>
auth-web-server page success-message text <success-message>
```

To set the type of logo appearing on the Web-Authentication page, use the commands below:

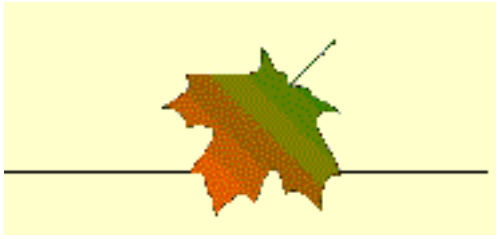
```
auth-web-server page logo {auto|default|hidden}
```

To display the custom logo if installed, use the **auto** parameter.
To display the default Allied Telesis globe logo, use the **default** parameter.
To hide the logo, use the **hidden** parameter.

You need to upload the custom logo to the flash of the device from an external storage media such as SD card, USB device or TFTP server. For example, to upload a custom logo from a TFTP server to the flash of the device, use the commands below:

```
copy tftp://<tftp server address>/my_logo.gif  flash:/logo.gif
```

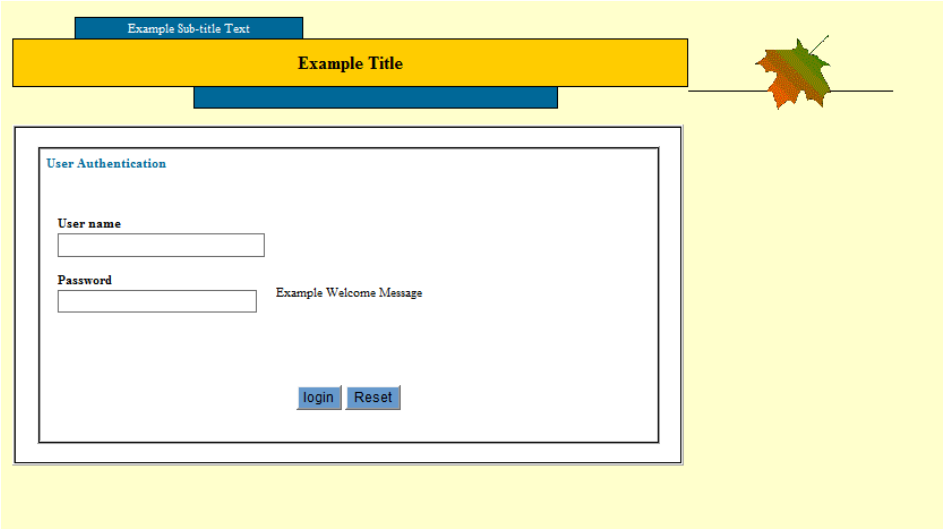
The logo file name must be logo.gif and the file format must be gif. The recommended dimension for the file is 185 X 90 pixels. The file must be stored in flash:/logo.gif on the device. An example logo is shown below:

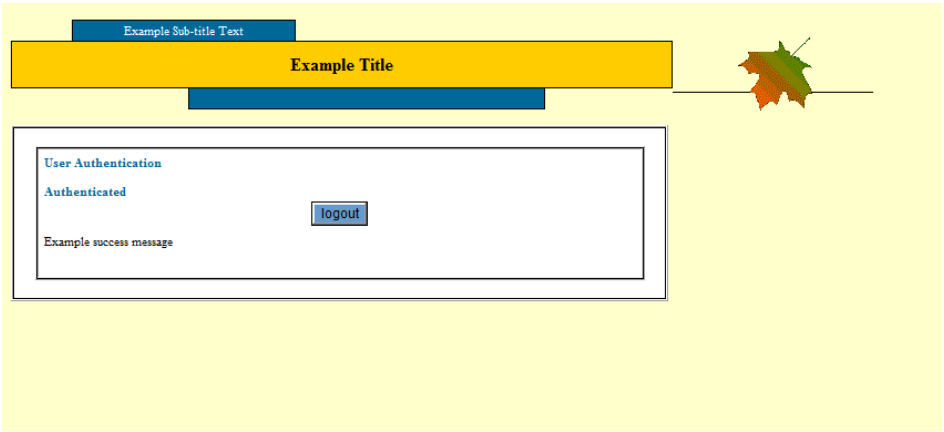


Use the following commands to customize the login page.

```
auth-web-server page sub-title text Example Sub-title Text
auth-web-server page title Example Title

auth-web-server page welcome-message text Example Welcome Message
auth-web-server page success-message text Example success Message
```

The custom Web-Authentication login page is displayed below:





Support for Protocols Underlying Web-Authentication

Web-Authentication does not use a dedicated protocol like 802.1X, with a standards-defined set of messages for authentication conversation. Instead, the switch overlays the Web-Authentication process on top of the web browser communication process. The browser communication process was not designed for authentication and is itself reliant on IP addressing, ARP, and DNS.

The authentication needs to occur in a seamless manner for all users, irrespective of their IP and DNS setting, and before they have full access to the network.

To make this possible, the switch needs to provide facilities that enable the user's PC to access the authentication web page.

Following features of Web-Authentication work together to achieve this.

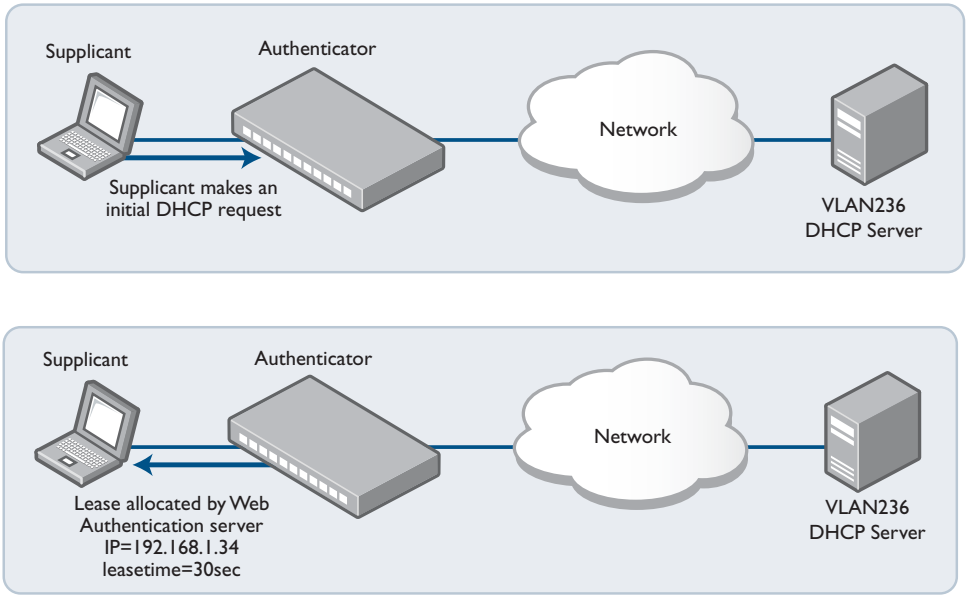
- DHCP server for Web-Authentication
- Interception of clients' ARPs
- Proxy DNS response

DHCP server for Web-Authentication

To initiate a web browsing session, the supplicant needs an IP address. If the supplicant has been configured to obtain its IP address by DHCP, then the authenticating switch needs to ensure that the supplicant will be served an IP address.

The simplest way to achieve this, is to have the Web-Authentication process itself act as a DHCP server. This avoids forwarding the supplicant's DHCP request to any other DHCP server. Therefore, there is a DHCP server built in to Web-Authentication.

This DHCP server is dedicated to serving IP addresses to be used by Web-Authentication clients.



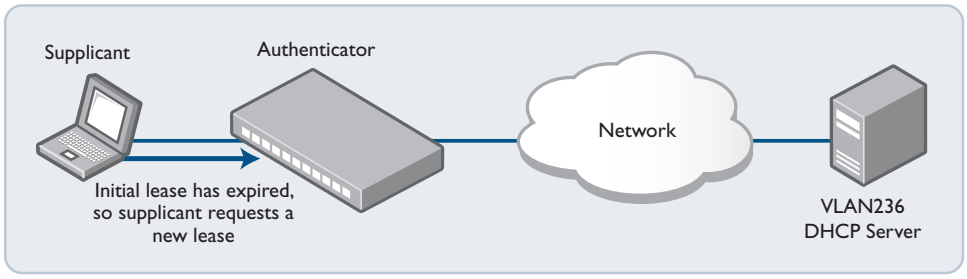
This DHCP service is configured by the command:

```
awplus(config)# auth-web-server dhcp ipaddress <ip-address/
                prefix-length>
```

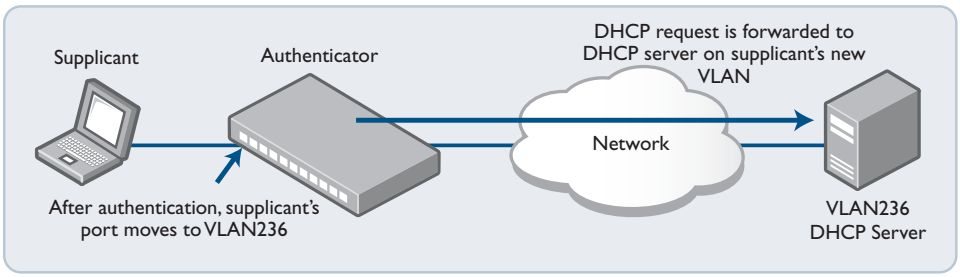
See the **auth-web-server dhcp ipaddress** command on page 43.41 and the **auth-web-server dhcp lease** command on page 43.42 for details about configuring the Web-Authentication DHCP Server.

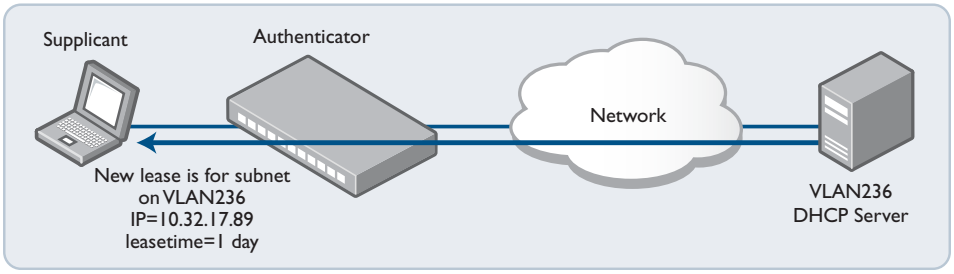
How can we force the supplicant to request a new DHCP lease after the completion of the authentication process? There is no mechanism by which the supplicant's web browser signals down to the DHCP client process to say "I've just completed an authentication session, so you need to request a new DHCP lease".

The solution is to ensure that the lease allocated by the dedicated Web-Authentication DHCP service is of a very short duration. This way the lease will expire within a short time from the completion of the authentication process, resulting in the supplicant requesting a new lease.



This new request will now be serviced by the DHCP server on the supplicant's new VLAN.

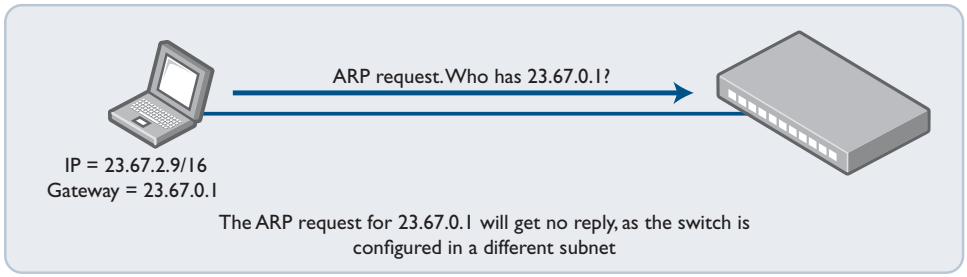




Interception of clients' ARPs

If the supplicant has been configured with a static IP address, then it is more than likely that the supplicant's IP configuration bears no relation to the Web-Authentication server address. A computer's IP communications will always be preceded by sending out ARP requests for host addresses in its local subnet, or for its gateway address.

If the IP address and gateway address have been statically configured on the computer, and the subnet used in this static configuration is different to that on the authenticating switch, then the ARP requests will receive no reply, and the PC will not begin IP communication.



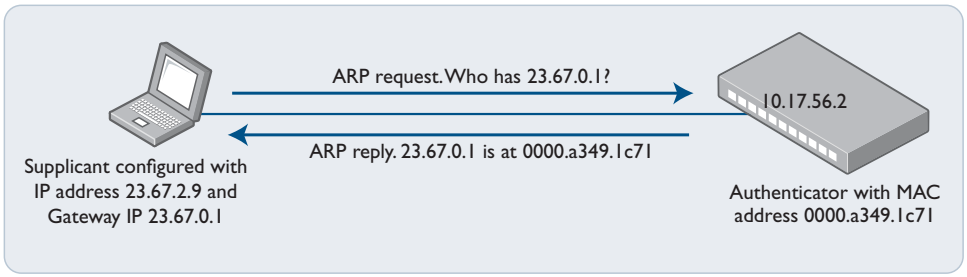
To deal with any arbitrary IP configuration on the supplicants, Web-Authentication needs a method for replying to arbitrary ARP requests. This is the ARP interception feature.

ARP interception can operate in three modes.

1. **Intercept** – will respond to ARP requests for any IP address that is in the same subnet as the switch's own IP address. Will provide its own MAC address in the ARP reply, irrespective of what IP address (within its own subnet) was being requested.

2. **None** – will only respond to ARP requests for its own IP address.

3. **Promiscuous** – will respond to **any** ARP request. Will provide its own MAC address in the ARP reply, irrespective of what IP address was being requested. When this mode is configured, the Web-Authentication server can interoperate with **any** static IP configuration on a supplicant.



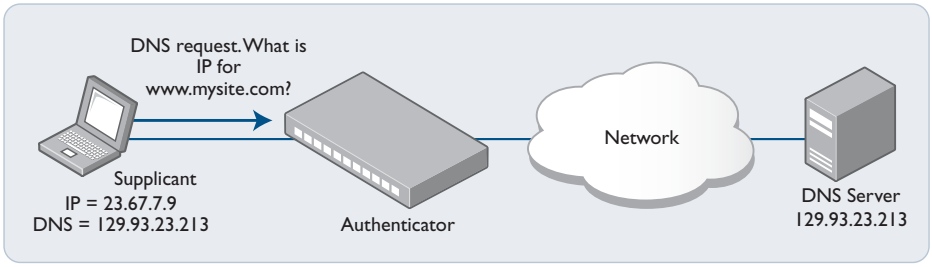
In promiscuous mode, the switch will send its own MAC address in response to an ARP request for ANY address, no matter whether the requested address bears any relation to the switch's own IP address on the interface where the ARP is received.

See the **auth-web-server mode (deleted)** command on page 43.50 for command information about setting the Web-Authentication mode.

Proxy DNS response

Typically, an HTTP session from a web browser is preceded by a DNS request for the IP address of the web site the user wishes to browse to. If the DNS request receives no reply, the web browser will never progress on to connecting an HTTP session.

The Web-Authentication server needs a mechanism to reply to DNS requests, so that the Web-Authentication session can begin.



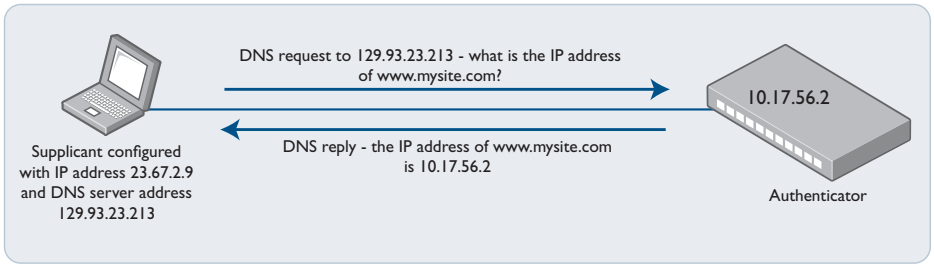
A web browser must request a DNS Server for the IP address corresponding to a URL. But the switch will not forward the request if the supplicant is not yet authenticated

The three modes listed also control the operation of the proxy DNS replies.

1. **Intercept** – responds to DNS requests whose source IP address is within the same subnet as the IP address on the switch. The IP address provided as the resolution of the DNS lookup is the switch's own IP address, so that the subsequent HTTP traffic will be directed to the switch.

2. **None** – the default. Does not respond to DNS requests.

3. **Promiscuous** – responds to DNS requests from any source IP address. The IP address provided as the resolution of the DNS lookup is the switch's own IP address, so that the subsequent HTTP traffic will be directed to the switch.



In promiscuous mode, the switch will reply to ANY DNS request from an authenticated supplicant, regardless of whether the destination IP address of the DNS server bears any relation to the switch's own IP address. The DNS reply from the switch will always specify its own IP address as the URL that was being requested.

See the **auth-web-server mode (deleted)** command on page 43.50 for command information about setting the Web-Authentication mode.

You can use the parameter <*ip-address*> of the **auth-web forward** command to specify a server for the switch to send packets from the supplicant to, for example DNS packets. For more information and an example, see the "Forwarding DNS packets using Auth-web forward command" section in the **Alliedware Plus Technical Tips and Tricks.**

Web-Authentication Timeout Connect

The command **auth timeout connect-timeout** allows you to increase the connection period for a supplicant's interface port.

The default timeout period is 30 seconds, but this command allows the timeout period to be set from 1 second to 65535 seconds. When **auth-web-server session-keep** or **auth two-step enable** is enabled, it is recommended to configure a longer connect-timeout period.

Web Authorization Proxy

Without this feature, AlliedWare Plus Web-Authentication intercepts a supplicant's initial TCP port 80 connection to a web page and sends it to the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation, use the command **auth-web-server intercept-port**.

When a supplicant is configured to use WPAD (Web Proxy Auto-Discovery) the supplicant's web browser will use TCP port 80 as usual, and so it can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page is sent. However, after authentication, it does not know where to get the WPAD file (usually named proxy.pac) that tells it what its web proxy is and so cannot access external web pages.

You can use the **auth-web-server dhcp-wpad-option** command to tell the supplicant where to find the proxy.pac file. This proxy.pac file contains the URL and/or IP address of the web proxy server that it should use.

For more information and examples, see the "Web Auth Proxy" section in the **Alliedware Plus Technical Tips and Tricks.**

MAC-Authentication

Why is MAC-Authentication Required?

The authentication mechanisms provided by 802.1X and Web-Authentication are powerful and effective. But, they are not universally applicable. Web-Authentication is only applicable to devices that have a human user who opens the web browser and types in a username and password when requested. 802.1X-Authentication is only possible from devices whose software implements an 802.1X supplicant.

There are plenty of network-connected devices, like printers, scanners, fire-alarm monitors and so on, that have neither a human user nor implement an 802.1X supplicant. In a network that ensures all access is authenticated, there needs to be a mechanism for authenticating these devices.

Fortunately, all Ethernet transceivers have a unique identifier—their MAC address. Hence, even without user input of a username and password, any Ethernet device will automatically identify itself simply by virtue of the source MAC address in the packets it sends. The method that has been developed for authenticating these devices uses the MAC address as the identifier, and so is called MAC-based authentication.

How Does MAC-Authentication Work?

In essence, MAC-authentication works little differently from 802.1X or Web-based authentication.

Here are the main steps:

1. The supplicant is connected to the switch.
2. The switch (acting as the authenticator) receives an ID from the supplicant.
3. The switch passes the supplicant's ID to a RADIUS server in an Access-Request packet
4. The RADIUS server returns an Access-Accept or an Access-Deny. The Access-Accept can be accompanied with other attributes, for dynamic VLAN assignment.

The unique aspects of MAC-Authentication are in steps 2 and 3.

MAC-Authentication does not involve a process whereby the switch sends an ID request to the supplicant. The switch receives the ID from the supplicant by simply looking at the source MAC in the packets being sent from the supplicant.

The MAC address of the supplicant is a single identifier. But a RADIUS access-request requires both a username and a password. The workaround employed by MAC-Authentication is simply to use the MAC address as both username and password.

The switch extracts the source MAC address from the supplicant's packets and puts it into a string of the form xx-xx-xx-xx-xx-xx, using lower-case letters for any hex digits in the range a-f. This string is then used as both the username and the password in the RADIUS access-request packet. The supplicant MAC address is also sent in the attribute 31 “calling-station-id” as usual.

Configuring MAC-Authentication

Under AlliedWare Plus, there are two steps to setting up MAC-Authentication.

1. Define the authentication method list that is used for MAC-Authentication.

There is only one method list that can be created for MAC-Authentication—the default method list. Moreover, the only authentication server type that can be used is RADIUS.

The command for defining the method list is:

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

2. Enable MAC-Authentication on the ports that are to perform this authentication:

```
awplus(config)# interface port1.0.2
awplus(config)# auth-mac enable
awplus(config)# spanning-tree edgeport
```

On the RADIUS server, it is necessary to create user entries where both the username and password are the MAC address of the supplicant, in the form xx-xx-xx-xx-xx-xx.

For example, on the AlliedWare Plus local RADIUS server, the configuration is:

```
          awplus(config)# radius-server local
  awplus(config-radsrv)# user xx-xx-xx-xx-xx-xx
                       password xx-xx-xx-xx-xx-xx
```

The supplicant requires no configuration, as the whole purpose of MAC-Authentication is to authenticate devices that cannot be configured for authentication.

It is also possible to configure the authentication protocol that the switch uses in its interaction with the RADIUS server. There are two choices of protocol: EAP-MD5 and PAP. The default method is PAP, and can be changed by using the command:

```
awplus(config-if)# auth-mac method [eap-md5|pap]
```

Tri-Authentication

The switch supports three types of authentication for devices that connect to switch ports.

- 802.1X-Authentication of devices connecting to switch ports
- MAC-Authentication of devices connecting to switch ports
- Web-Authentication of devices connecting to switch ports

All three types can be configured to run simultaneously on a switch port. The simultaneous configuration and authentication of all three types on a port is called tri-authentication.

Tri-Authentication Configuration

Follow the below three steps to configure tri-authentication across a range of switch ports:

Step 1: Define the RADIUS Server:

Define the RADIUS Server where the switch will send authentication requests by using the below commands:

```
awplus# configure terminal
awplus(config)# radius-server host <ip-address> key
<key-string>
```

These commands adds the RADIUS Server address and set parameters to the RADIUS server. The key parameter specifies the secret key for the server.

Step 2: Define the default authentication server lists:

Define the default authentication server lists for 802.1X-Authentication, Web-Authentication, and MAC-Authentication:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x default group radius
awplus(config)# aaa authentication auth-web default group
radius
awplus(config)# aaa authentication auth-mac default group
radius
```

Step 3: Enable 802.1X-Authentication, Web-Authentication, and MAC-Authentication:

Follow the instructions below to enable 802.1X-Authentication, Web-Authentication, and MAC-Authentication on switch ports to attach supplicant devices. This authenticates the supplicant if any of the three methods that the supplicant tries work, depending on the auth-fail VLAN settings. After enabling the authentication, refer to earlier chapters to configure VLAN, IP address and other authentication configurations for the authentication type you want.

```
awplus# configure terminal
awplus(config)# interface <interface-range>
awplus(config-if)# switchport mode access
awplus(config-if)# switchport access vlan 1
awplus(config-if)# auth-web enable
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
```

Two-Step Authentication

The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device
- an authorized user can access the network with an unauthorized device

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

The following authentication sequences are supported for two-step authentication:

MAC-Authentication followed by 802.1X-Authentication

MAC-Authentication followed by Web-Authentication

802.1X-Authentication followed by Web-Authentication.

To configure two-step authentication:

1. Configure the first authentication method.
2. Configure the second authentication method.
3. Specify the command **auth two-step enable**.
4. Make sure that both authentication steps require different authentication credentials. See **"Ensuring Authentication Methods Require Different Usernames and Passwords" on page 42.28**.

For more information and examples, see the "Two-step authentication" section in the **Alliedware Plus Technical Tips and Tricks.**

Ensuring Authentication Methods Require Different Usernames and Passwords

If you configure a user or device to use multiple authentication methods, you need to set up your system to avoid a potential vulnerability.

The vulnerability occurs because there is no way for a RADIUS server to determine what authentication method you are using. Authentication simply queries a RADIUS server to see whether a username/password pair is valid.

This means that if you use the same RADIUS server for multiple authentication methods, a user can enter the *same* username/password pair for each of these authentication methods. If that username/password pair is valid for one of the methods, it will work for all of them.

This vulnerability is particularly significant for MAC-Authentication, because the default username and password is the MAC address of the supplicant device, which is easy to discover.

For example, if you set up two-step authentication of MAC-Authentication and 802.1X-Authentication, and both use the same RADIUS server, then an attacker does not need to know the 801.1x username and password. Instead, they can pass the 802.1X-Authentication step by entering the device's MAC address into the 802.1X username and password fields.

To avoid this vulnerability:

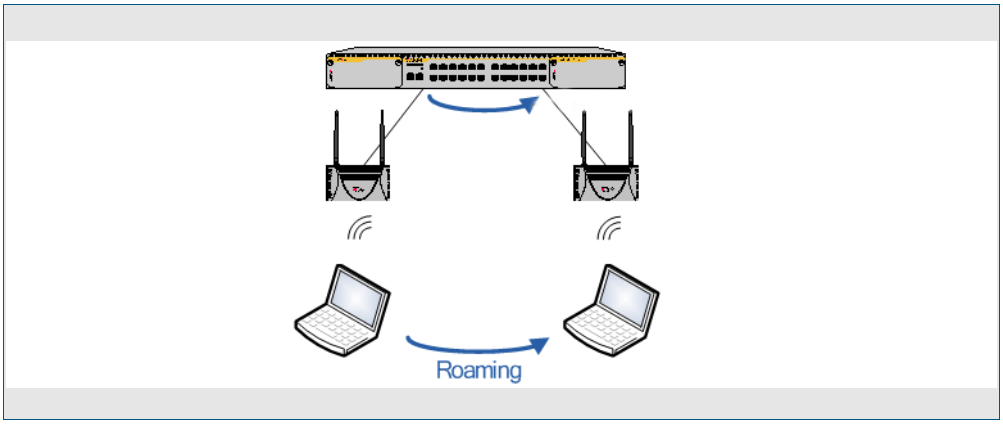
- Use different RADIUS servers for each authentication method, and/or
- Change the default password for MAC-Authentication, by using the **auth-mac password** command on page 43.33.

Roaming Authentication

When network security is required, the usability of network security must be considered. The Roaming Authentication feature improves the usability of network security by enabling users to move within the network without requiring them to re-authenticate each time they move.

If a supplicant (client device) moves from one wireless access point to another wireless access point, and the wireless access points are connected to different ports, then the switch (authenticator) recognizes that the supplicant has been authenticated and accepts the supplicant without requiring re-authentication.

Figure 42-1: Diagram showing Roaming Authentication running on a standalone switch

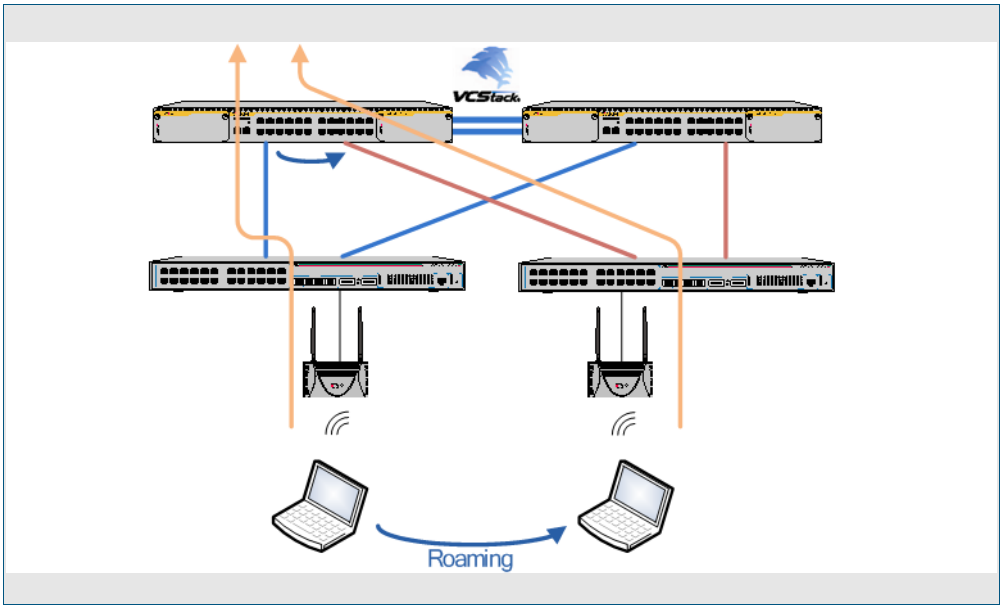


Web-Authentication and MAC-Authentication are the authentication methods in a Wireless LAN environment, and 802.1X is the authentication method used for supplicants attached to edge switches.

Roaming Authentication is normally enabled using the **auth roaming enable** command on page 43.19 command. However, Roaming Authentication has been extended (with the **auth roaming disconnected** command on page 43.17) to work where an interface is link down. This allows you to enable supplicants to move from authenticated interfaces that are link down, without requiring re-authentication.

Roaming Authentication is available for use with the VCStack feature, and is available on static and dynamic (LACP) channel group interfaces.

Figure 42-2: Diagram showing Roaming Authentication running with VCStack



Roaming Authentication Overview

If the Roaming Authentication feature is **disabled** and a supplicant moves from one switchport to another, the supplicant's authenticated status, authentication, and assigned VLAN are deleted. The supplicant is re-authenticated at the new switchport so that the network can be accessed. While the supplicant is being re-authenticated, all traffic from the supplicant is dropped.

When the Roaming Authentication feature is **enabled**, a new switch port inherits the status of a supplicant from the switch port that the supplicant moved from. If the Roaming Authentication feature is enabled on a switch, then once a supplicant (client device) is authenticated on the switch it does not have to be re-authenticated if it moves between the ports of that switch. Supplicant traffic is not dropped because there is no delay for re-authentication, during which the supplicant would be unable to access the network.

For example, when the Roaming Authentication feature is used in a wireless LAN environment with wireless access points, the wireless clients can roam between wireless access points connected to different switch ports without re-authentication.

The Roaming Authentication feature also supports VCStack operation and works on defined static channel group (static aggregators) and dynamic channel group (LACP) interfaces. When VCStack and Roaming Authentication features are used together, the status of a supplicant is inherited from one aggregated interface to another aggregated interface over the stack.

See the **auth roaming disconnected** command on page 43.17 and the **auth roaming enable** command on page 43.19 for further information about configuring Roaming Authentication.

Roaming Authentication Feature Interactions

When the Roaming Authentication feature is disabled, a supplicant must be re-authenticated on the destination interface when it roams. When the Roaming Authentication is enabled, the following supplicant authentication status and information is inherited from the source interface:

- Authentication status
- Authentication method
- Supplicant MAC address
- Supplicant IP address
  (if an authenticated interface is configured for Web-Authentication)
- Supplicant name
- Authorized dynamic VLAN ID
- Authorized RADIUS server
- Reauthentication timer
  (if configured using the **auth timeout reauth-period** command on page 43.25)

Roaming Authentication is only supported between interfaces with the same authentication configuration. If source and destination interfaces have different authentication configuration then the supplicant will be re-authenticated at the destination interface.

When the host mode is set with the **auth host-mode** command on page 43.11, a supplicant is not authenticated on a destination interface, and the authentication status is deleted on the source interface.

When a supplicant moves from an interface with authentication configured to an interface without authentication configured, the supplicant's authentication status is deleted.

A supplicant is re-authenticated when it moves to a destination interface that is configured on a different VLAN than the VLAN that is configured for the source interface.

See the following Roaming Authentication feature interactions:

- Multiple Dynamic VLANs are supported when configured with the **auth dynamic-vlan-creation** command on page 43.6 using the **multi** parameter. Multiple Dynamic VLANs are disabled by default.
- Supplicants are re-authenticated on the destination interface if the VLAN ID changes when Single Dynamic VLANs are configured with the **auth dynamic-vlan-creation** command on page 43.6 the using the **single** parameter. Single Dynamic VLANs are disabled by default.
- The Roaming Authentication feature is supported on Guest VLANs configured by the **auth guest-vlan** command on page 43.9.

When the Roaming Authentication feature is configured for use on a stack with the VCStack feature, note that supplicants are initialized and re-authenticated if a VCStack failover occurs.

Unauthenticated Supplicant Traffic

When any authentication is configured on a switch port, the question arises as to what the switch does with packets that arrive into the switch port from unauthenticated supplicants.

Unauthenticated supplicants fall into three categories listed below:

- Newly attached supplicants, which are still in the process of their first authentication attempt
- Supplicants that have made an authentication attempt, but have failed authentication
- Supplicants that have been attached, but have not made an authentication attempt. For example, on a port that has only 802.1X-Authentication enabled, any supplicant that has no 802.1X client software will not be able to attempt 802.1X-Authentication.

In switches that are running the AlliedWare Plus™ Operating System, packets from all these three categories of unathenticated supplicants are treated equally; no distinction is made between these three categories. The treatment of the traffic from unauthenticated supplicants does, however, depend on two factors:

- Whether a Guest VLAN has been configured on the switch port to which the supplicant is attached
- Whether Web-Authentication has been configured on the switch port to which the supplicant is attached

The rules governing the treatment of packets from unauthenticated supplicants are laid out in the table below:

Table 42-1: Treatment of packets from unauthenticated supplicants

Switch port configuration	No Guest VLAN configured	No Guest VLAN configured, auth-fail VLAN configured	Guest VLAN configured
Web-Authentication configured	Packets from unauthenticated supplicants are associated with the Native VLAN of the port. Packets from unauthenticated supplicants are processed according these rules: ■ Packets destined to the WebAuth server IP address/ TCP port are forwarded to the server (which may well be the switch itself). ■ DHCP packets are sent to the CPU, to be processed by a local DHCP server, or relayed to another DHCP server, depending on the configuration of the switch. ■ DNS packets are forwarded to the CPU, and then sent on to a DNS server, if the switch is configured with a DNS server address. ■ ARP packets are forwarded to the CPU, and an ARP entry for the supplicant is learned. ■ If web-auth forwarding is enabled for particular types of packets, then those packets will be forwarded within the Native VLAN ■ All other packets are dropped.	Packets from unauthenticated supplicants are associated with the Native VLAN of the port. If newly connected supplicants attempt 802.1X port authentication or Web-Authentication and fail, then they are moved to the auth-fail VLAN.	Packets from unauthenticated supplicants are associated with the Guest VLAN of the port. Packets from unauthenticated supplicants are processed according to these rules: ■ Packets destined to the WebAuth server IP address/ TCP port are forwarded to the server (which may well be the switch itself). ■ DHCP packets are sent to the CPU, to be processed by a local DHCP server, or relayed to another DHCP server, depending on the configuration of the switch. ■ DNS packets are forwarded to the CPU, and then sent on to a DNS server, if the switch is configured with a DNS server address. ■ ARP packets are forwarded to the CPU, and an ARP entry for the supplicant is learned. ■ Drop all other packets destined to the IP address of the Guest VLAN. ■ Layer 2 forward packets destined to other addresses within the Guest VLAN. ■ All other packets are dropped.
No Web-Authentication configured	All non-eap packets from unauthenticated supplicants are dropped.	All non-eap packets from unauthenticated supplicants are dropped.	Packets from unauthenticated supplicants are associated with the Guest VLAN of the port. The packets are processed according to these rules: ■ Drop packets destined to the IP address of the Guest VLAN. ■ Layer 2 forward packets destined to other addresses within the Guest VLAN. ■ Drop all other packets.

Deciding When a Supplicant Fails Authentication

Although the treatment of packets from unauthenticated supplicants does not differentiate between the three categories of supplicant, it is still useful to know for sure when the switch decides that a supplicant has failed authentication.

The rules for deciding that a supplicant has failed authentication are listed below for each type of authentication available:

Deciding when a supplicant fails 802.1X-Authentication

If the supplicant responds to EAP authentication requests, and the supplicant's authentication information is sent to the RADIUS server, and the RADIUS server replies with an Authentication-Reject, then the supplicant is immediately deemed to have failed authentication.

If the supplicant does not respond to EAP authentication requests, then the switch will resend the authentication requests up to a maximum number of attempts set by the command **dot1x max-reauth-req** (the default is 2). The interval between the attempts is set by the command **dot1x timeout tx-period** (the default is 30 seconds). If the supplicant still has not responded after this, it is deemed to have not attempted authentication.

See **Chapter 47, 802.1X Commands** for 802.1X-Authentication command information.

Deciding when a supplicant fails Web-Authentication

As soon as the supplicant attempts any web-browsing, the switch will intercept the web session, and present the supplicant with an authentication request page. If the user enters a username and password, and clicks the login button, then the switch will send the username and password to the RADIUS server. If the RADIUS server replies with an Authentication-Reject, then the supplicant is immediately deemed to have failed authentication.

Until the supplicant has attempted any web-browsing, or has received the authentication request page, but not yet clicked the login button, the supplicant is deemed to be not yet authenticated (as against not able to authenticate).

See **Chapter 43, Authentication Commands** for Web-Authentication command information.

Deciding when a supplicant fails MAC-Authentication

As soon as the supplicant sends any packet, the source MAC address from the packet will be sent to the RADIUS server for authentication. If the RADIUS server replies with an Authentication-Reject, then the supplicant is immediately deemed to have failed authentication.

With MAC-Authentication there really is no concept of not-yet-attempted authentication, because authentication is attempted as soon as a supplicant sends a packet.

See **Chapter 43, Authentication Commands** for MAC-Authentication command information.

Failed Authentication VLAN

The auth-fail VLAN feature allows the network administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication.

This feature enables the network administrator to enact a security policy in which the supplicants who fail authentication are given extremely limited access, or are given access to remedial applications.

If the Guest VLAN and auth-fail VLAN are both configured on a switch, then a newly connected supplicant initially belongs to the Guest VLAN. If newly connected supplicants attempt 802.1X port authentication or Web-Authentication and fail, then they are moved from the Guest VLAN to the auth-fail VLAN.

The criteria for how many failed authentication attempts are allowed before the supplicant is moved to the auth-fail VLAN differs, depending on the authentication method used.

If Web-Authentication is used, then the supplicant is moved to the auth-fail VLAN after the first failed attempt. If 802.1X port authentication is used, then the supplicant is moved to the auth-fail VLAN after the number of failed attempts is equal to the value configured by the dot1x max-auth-fail command (by default, three failed 802.1X-Authentication attempts are allowed).

The MAC-Authentication feature does not support the max-auth-fail option. If auth-fail VLAN feature is used in conjunction with MAC-Authentication only one attempt is allowed for a MAC-Authentication supplicant. If the attempt fails, then the supplicant will be treated as "Authenticated" and the interface will be added to the configured auth-fail VLAN.

Limitations on Allowed Feature Combinations

Note that the Web-Authentication feature cannot be used with the Guest VLAN or auth-fail VLAN features. For further limitation information see the below tables:

Table 42-2: Interoperation of authentication types with guest VLAN and auth-fail VLAN

Authentication Type	Guest VLAN (without routing mode)	Guest VLAN (with routing mode)	Failed Authentication VLAN
802.1X-Authentication	Layer 2 forward packets destined to other addresses within the Guest VLAN.	Unauthorized supplicant can access Guest VLAN. Use ACL for security on the interface.	Failed authentication supplicant can access auth-fail VLAN. See limitations table below for ACL usage limitation.
MAC-Authentication	Layer 2 forward packets destined to other addresses within the Guest VLAN.	Unauthorized supplicant can access Guest VLAN. Use ACL for security on the interface.	Failed authentication supplicant can access auth-fail VLAN. See limitations table below for ACL usage limitation.
Web-Authentication (without intercept mode)	Layer 2 forward packets destined to other addresses within the Guest VLAN.	Unauthorized supplicant can access Guest VLAN. Use ACL for security on the interface.	Failed authentication supplicant can access auth-fail VLAN. See limitations table below for ACL usage limitation.
Web-Authentication (with intercept mode)	(Not Available)	(Not Available)	(Not Available)

Table 42-3: Interactions between guest VLAN and auth-fail VLAN

Authentication Feature	Guest VLAN (without routing mode)	Guest VLAN (with routing mode)	Failed Authentication VLAN
Guest VLAN (without routing mode)	(Not Available)	(Not Available)	Cannot configure ACLs on the Guest VLAN when it is not in routing mode. The Guest VLAN without routing mode has reserved ACLs already attached to it.
Guest VLAN (with routing mode)	(Not Available)	(Not Available)	Configuration of ACLs for additional interface security is recommended.
Failed Authentication VLAN	Cannot configure ACLs on the Guest VLAN when it is not in routing mode. The Guest VLAN without routing mode has reserved ACLs already attached to it.	Configuration of ACLs for additional interface security is recommended.	Failed authentication supplicant can access auth-fail VLAN. See limitations table below for ACL usage limitation.

Chapter 43: Authentication Commands

Command List 43.3
auth auth-fail vlan 43.3
auth critical 43.5
auth dynamic-vlan-creation 43.6
auth guest-vlan 43.9
auth host-mode 43.11
auth log 43.13
auth max-supplicant 43.15
auth reauthentication 43.16
auth roaming disconnected 43.17
auth roaming enable 43.19
auth supplicant-mac 43.21
auth timeout connect-timeout 43.23
auth timeout quiet-period 43.24
auth timeout reauth-period 43.25
auth timeout server-timeout 43.26
auth timeout supp-timeout 43.27
auth two-step enable 43.28
auth-mac enable 43.31
auth-mac method 43.32
auth-mac password 43.33
auth-mac reauth-relearning 43.34
auth-web enable 43.35
auth-web forward 43.36
auth-web max-auth-fail 43.38
auth-web method 43.39
auth-web-server blocking-mode 43.40
auth-web-server dhcp ipaddress 43.41
auth-web-server dhcp lease 43.42
auth-web-server dhcp-wpad-option 43.43
auth-web-server gateway (deleted) 43.44
auth-web-server host-name 43.45
auth-web-server http-redirect (deleted) 43.46
auth-web-server intercept-port 43.47
auth-web-server ipaddress 43.48
auth-web-server login-url 43.49
auth-web-server mode (deleted) 43.50
auth-web-server page logo 43.51
auth-web-server page sub-title 43.52
auth-web-server page success-message 43.53
auth-web-server page title 43.54
auth-web-server page welcome-message 43.55
auth-web-server ping-poll enable 43.56
auth-web-server ping-poll failcount 43.57
auth-web-server ping-poll interval 43.58
auth-web-server ping-poll reauth-timer-refresh 43.59
auth-web-server ping-poll timeout 43.60

auth-web-server port....43.61
auth-web-server redirect-delay-time....43.62
auth-web-server redirect-url....43.63
auth-web-server session-keep....43.64
auth-web-server ssl....43.65
auth-web-server sslport (deleted)....43.66
auth-web-server ssl intercept-port....43.67
copy proxy-autoconfig-file....43.68
copy web-auth-https-file....43.68
erase proxy-autoconfig-file....43.69
erase web-auth-https-file....43.69
show auth two-step supplicant brief....43.70
show auth-mac....43.71
show auth-mac diagnostics....43.72
show auth-mac interface....43.73
show auth-mac sessionstatistics....43.76
show auth-mac statistics interface....43.77
show auth-mac supplicant....43.78
show auth-mac supplicant interface....43.80
show auth-web....43.81
show auth-web diagnostics....43.83
show auth-web interface....43.84
show auth-web sessionstatistics....43.87
show auth-web statistics interface....43.88
show auth-web supplicant....43.89
show auth-web supplicant interface....43.90
show auth-web-server....43.91
show auth-web-server page....43.92
show proxy-autoconfig-file....43.93

Command List

This chapter provides an alphabetical reference for authentication commands.

auth auth-fail vlan

Use this command to enable the **auth-fail vlan** feature on the specified vlan interface. This feature assigns supplicants (client devices), which have failed port authentication, to the specified VLAN interface.

Use the **no** variant of this command to disable the **auth-fail vlan** feature for a specified VLAN interface.

Syntax

```
auth auth-fail vlan <1-4094>
no auth auth-fail vlan
```

Parameter	Description
<1-4094>	Assigns the VLAN ID to any supplicants that have failed port authentication.

Default The **auth-fail vlan** feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use the **auth-fail vlan** feature when using Web-Authentication instead of the Guest VLAN feature, when you need to separate networks where one supplicant (client device) requires authentication and another supplicant does not require authentication from the same interface.

This is because the DHCP lease time using the Web-Authentication feature is shorter, and the **auth fail vlan** feature enables assignment to a different VLAN if a supplicant fails authentication.

To enable the **auth-fail vlan** feature with Web Authentication, you need to set Web Authentication Server virtual IP address by using the **auth-web-server ipaddress** command on page 43.48 or the **auth-web-server dhcp ipaddress** command on page 43.41.

When using 802.1X port authentication, use a **dot1x max-auth-fail** command to set the maximum number of login attempts. Three login attempts are allowed by default for 802.1X port authentication before supplicants trying to authenticate are moved from the Guest VLAN to the auth-fail VLAN. See the **"dot1x max-auth-fail" on page 47.9** for command information.

See the section **"Failed Authentication VLAN" on page 42.35** in **Chapter 42, Authentication Introduction and Configuration** for further overview information about the auth-fail VLAN feature, which allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication.

See the section **"Limitations on Allowed Feature Combinations" on page 42.35** for information about restrictions regarding combinations of authentication enhancements working together.

Use appropriate ACLs (Access Control Lists) on interfaces for extra security if a supplicant allocated to the designated auth-fail vlan can access the same network as a supplicant on the Guest VLAN. For more information about ACL concepts, and configuring ACLs see **Chapter 36, Access Control Lists Introduction**. For more information about ACL commands see:

- **Chapter 37, IPv4 Hardware Access Control List (ACL) Commands**
- **Chapter 38, IPv4 Software Access Control List (ACL) Commands**
- **Chapter 39, IPv6 Software Access Control List (ACL) Commands**

Examples

To enable **auth-fail vlan** for `port1.0.2` and assign VLAN `100`, use the following commands:

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

To disable the **auth-fail vlan** feature for `port1.0.2`, use the following commands:

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

Validation Commands

show running-config

Related Commands

dot1x max-auth-fail
show dot1x
show dot1x interface

auth critical

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

The **no** variant of this command disables critical port feature on the interface.

Syntax

```
auth critical
no auth critical
```

Default The critical port of port authentication is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To enable the critical port feature on interface `port1.0.2`, use the following commands:

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

To disable the critical port feature on interface `port1.0.2`, use the following commands:

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

Validation Commands

show auth-web-server
show dot1x
show dot1x interface
show running-config

auth dynamic-vlan-creation

This command enables and disables the Dynamic VLAN assignment feature.

The Dynamic VLAN assignment feature allows a supplicant (client device) to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given interface.

Use the **no** variant of this command to disable the Dynamic VLAN assignment feature.

Syntax

```
auth dynamic-vlan-creation [rule {deny|permit}] [type {multi|single}]
no auth dynamic-vlan-creation
```

Parameter	Description
`rule`	VLAN assignment rule.
`deny`	Deny a differently assigned VLAN ID. This is the default rule.
`permit`	Permit a differently assigned VLAN ID.
`type`	Specifies whether multiple different VLANs can be assigned to supplicants (client devices) attached to the port, or whether only a single VLAN can be assigned to supplicants on the port.
`multi`	Multiple Dynamic VLAN.
`single`	Single Dynamic VLAN.

Default By default, the Dynamic VLAN assignment feature is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage If the Dynamic VLAN assignment feature is enabled (disabled by default), VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports. Dynamic VLANs may be associated with authenticated MAC addresses if the **type** parameter is applied with the **rule** parameter.

The **rule** parameter deals with the case where there are multiple supplicants attached to a port, and the type parameter has been set to **single-vlan**. The parameter specifies how the switch should act if different VLAN IDs end up being assigned to different supplicants. The keyword value **deny** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is rejected. The keyword value **permit** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is accepted, but it is actually assigned the same VID as the first supplicant.

If you issue an **auth dynamic-vlan-creation** command without an optional **rule** parameter and a required **deny** or **permit** keyword value then a second supplicant with a different VLAN ID is rejected. It is not assigned to the first supplicant's VLAN. Issuing an a**uth dynamic-vlan-creation** command without an optional **rule** parameter has the same effect as issuing an **auth dynamic-vlan-creation rule deny** command rejecting supplicants with differing VIDs.

The **type** parameter specifies whether multiple different VLANs can be assigned to supplicants attached to the port, or whether only a single VLAN can be assigned to

supplicants on the port. The **type** parameter can select the port base VLAN or the MAC base VLAN from the RADIUS VLAN ID. This can be used when the host-mode is set to multi-supplicant. For **single**-host ports, the VLAN ID will be assigned to the port. It is not supported with the Guest VLAN feature. Display the ID assigned using a **show vlan** command. For **multi**-host ports, the VLAN ID will be assigned to the MAC address of the authenticated supplicant. The VLAN ID assigned for the MAC Base VLAN is displayed using the **show platform table vlan** command.

To configure Dynamic Vlan with Web Authentication, you need to set Web Authentication Server virtual IP address by using the **auth-web-server ipaddress** command on page 43.48 or the **auth-web-server dhcp ipaddress** command on page 43.41. You also need to create a hardware access-list that can be applied to the switch port interface.

You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

Examples To enable the Dynamic VLAN assignment feature on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 10
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# interface vlan10
awplus(config-if)# ip address 10.1.1.1/24
```

To enable the Dynamic VLAN assignment feature with Web Authentication on interface `port1.0.2` when Web Authentication is needed, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 1.2.3.4
awplus(config)# access-list hardware acl-web send-
                to-cpu ip any 1.2.3.4
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# access-group acl-web
awplus(config-if)# interface vlan1
awplus(config-if)# ip address 10.1.1.1/24
```

To disable the Dynamic VLAN assignment feature on interface `port1.0.2`, use the commands:

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

Validation Commands

show dot1x
show dot1x interface
show running-config

Related Commands

auth host-mode

auth guest-vlan

This command enables and configures the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. This command does not start authentication. The supplicant's (client device's) traffic is associated with the native VLAN of the interface if its not already associated with another VLAN. The **routing** option enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.

The **no** variant of this command disables the guest vlan feature on the interface specified.

Syntax

```
auth guest-vlan <1-4094> [routing]
no auth guest-vlan [routing]
```

Parameter	Description
<1-4094>	VLAN ID (VID).
`routing`	Enables routing from the Guest VLAN to other VLANs.

Default The Guest VLAN authentication feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

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

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

Note that you must first define the VLAN with the **vlan** command that you will assign as a guest VLAN using this command. Also note that 802.1X must first be enabled on the port.

Guest VLAN authentication cannot be enabled if DHCP snooping is enabled (**service dhcp-snooping** command on page 56.24), and vice versa.

The Guest VLAN feature in previous releases had some limitations that have been removed. Until this release the Guest VLAN feature could not lease the IP address to the supplicant using DHCP Server or DHCP Relay features unless Web-Authentication was also applied. When using NAP authentication, the supplicant should have been able to log on to a domain controller to gain certification, but the Guest VLAN would not accept access to another VLAN.

The Guest VLAN routing mode in this release overcomes these issues. With the Guest VLAN routing mode, the switch can lease DHCP addresses and accept access to a limited network.

Note that Guest VLAN can use only untagged ports and tagged ports cannot be used for Guest VLAN.

See the section **"Configuring a Guest VLAN" on page 42.2** for information about the Guest VLAN feature.

See the section **"Limitations on Allowed Feature Combinations" on page 42.35** for information about restrictions regarding combinations of authentication enhancements working together.

Examples To define `vlan100` and assign the guest VLAN feature to `vlan100` on interface `port1.0.2`, and enable routing from the guest vlan to other VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 100 routing
```

To disable the guest vlan feature on interface `port1.0.2`, use the following commands:

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

Validation Commands
show dot1x
show dot1x interface
show running-config

Related Commands
dot1x port-control
vlan

auth host-mode

This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X.

Use the **no** variant of this command to set host mode to the default setting (single host).

Syntax

```
auth host-mode {single-host|multi-host|multi-supplicant}
no auth host-mode
```

Parameter	Description
`single-host`	Single host mode. In this mode, only one host may be authorized with the port. If other hosts out the interface attempt to authenticate, the authenticator blocks the attempt.
`multi-host`	Multi host mode. In this mode, multiple hosts may be authorized with the port; however only one host must be successfully authenticated at the Authentication Server for all hosts to be authorized with the port. Upon one host being successfully authenticated (state Authenticated), the other hosts will be automatically authorized at the port (state ForceAuthorized). If no host is successfully authenticated, then all hosts are not authorized with the port.
`multi-supplicant`	Multi supplicant (client device) mode. In this mode, multiple hosts may be authorized with the port, but each host must be individually authenticated with the Authentication Server to be authorized with the port. Supplicants which are not authenticated are not authorized with the port, while supplicants which are successfully authenticated are authorized with the port.

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

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Ports residing in the unauthorized state for host(s) or supplicant(s), change to an authorized state when the host or supplicant has successfully authenticated with the Authentication Server.

When multi-host mode is used or auth critical feature is used, all hosts do not need to be authenticated.

Examples To set the host mode to multi-supplicant on interface `port1.0.2`, use the following commands:

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

To set the host mode to default (single host) on interface `port1.0.2`, use the following

commands:

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

Validation Commands

show dot1x
show dot1x interface
show running-config

auth log

Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the **no** variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

Syntax

```
auth log {dot1x|auth-mac|auth-web} {success|failure|logoff|all}
no auth log {do1x|auth-mac|auth-web} {success|failure|logoff|all}
```

Parameter	Description
`dot1x`	Specify only 802.1X-Authentication log messages are output to the log file.
`auth-mac`	Specify only MAC-Authentication log messages are output to the log file.
`auth-web`	Specify only Web-Authentication log messages are output to the log file.
`success`	Specify only successful authentication log messages are output to the log file.
`failure`	Specify only authentication failure log messages are output to the log file.
`logoff`	Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.
`all`	Specify all types of authentication log messages are output to the log file Note that this is the default behavior for the authentication logging feature.

Default All types of authentication log messages are output to the log file by default.

Mode Interface Configuration

Examples To configure the logging of MAC-Authentication failures to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

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

To configure the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

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

Validation Commands **show running-config**

auth max-supplicant

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

The **no** variant of this command resets the maximum supplicant number to the default (1024).

Syntax

```
auth max-supplicant <2-1024>
no auth max-supplicant
```

Parameter	Description
<2-1024>	Limit number.

Default The max supplicant of port authentication is 1024.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the maximum number of supplicants to `10` on interface `port1.0.2`, use the following commands:

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

To reset the maximum number of supplicant to default on interface `port1.0.2`, use the following commands:

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

Validation Commands

show dot1x
show dot1x interface
show running-config

auth reauthentication

This command enables re-authentication on the interface specified in the Interface mode, which may be a static channel group (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the **no** variant of this command to disables reauthentication on the interface.

Syntax

```
auth reauthentication
no auth reauthentication
```

Default Reauthentication of port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To enable reauthentication on interface `port1.0.2`, use the following commands:

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

Validation Commands

show dot1x
show dot1x interface
show running-config

auth roaming disconnected

This command enables the Roaming Authentication feature on an authenticated interface that is link down. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the **auth roaming enable** command before using this command. The **auth roaming disconnected** command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the **auth roaming enable** command.

The **no** variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See **"Web-Authentication" on page 42.4** for further information about this feature.

Syntax

```
auth roaming disconnected

no auth roaming disconnected
```

Default The Roaming Authentication `disconnected` feature is disabled by default on an interface. Authentication status for a roaming supplicant is deleted by default when an interface goes down.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage This command allows a supplicant to move to another authenticating interface without reauthentication, if the link is down for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure **auth roaming enable** on an interface before configuring **auth roaming disconnected** if you require **auth roaming disconnected** configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (**service dhcp-snooping** command on page 56.24), and vice versa.

Examples To enable Roaming Authentication `disconnected` feature for `port1.0.2`, after enabling 802.1X-Authentication and enabling Roaming Authentication `enable`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
awplus(config-if)# auth roaming disconnected
```

To disable Roaming Authentication disconnected feature for `port1.0.2`, use the commands:

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

Validation Commands

show running-config

Related Commands

auth-mac enable
auth roaming enable
auth-web enable
dot1x port-control
show auth-mac interface
show auth-web interface
show dot1x interface

auth roaming enable

This command enables the Roaming Authentication feature on an authenticated interface that is link up. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the **auth roaming enable** command before using **auth roaming disconnected** command. The **auth roaming disconnected** command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the **auth roaming enable** command.

The **no** variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See **"Web-Authentication" on page 42.4** for further information about this feature.

Syntax

```
auth roaming enable
no auth roaming enable
```

Default The Roaming Authentication enable feature is disabled by default on an interface.

Authentication status for a roaming supplicant is deleted by default when an interface goes down.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage This command allows a supplicant to move to another authenticating interface without reauthentication, providing the link is up for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure **auth roaming enable** on an interface before configuring **auth roaming disconnected** if you require **auth roaming disconnected** configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (**service dhcp-snooping** command on page 56.24), and vice versa.

Examples To enable the Roaming Authentication enable feature for interface `port1.0.4`, after enabling 802.1X-Authentication, since an authentication method is required, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
```

To disable Roaming Authentication enable for `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no auth roaming enable
```

Validation Commands

show running-config

Related Commands

auth-mac enable
auth roaming disconnected
auth-web enable
dot1x port-control
show auth-mac interface
show auth-web interface
show dot1x interface

auth supplicant-mac

This command adds a supplicant (client device) MAC address on a given interface with the parameters as specified in the table below.

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

Syntax

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

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

Parameter	Description
<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.
`skip-second-auth`	Skip the second authentication.
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout (default 30 seconds).
<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 Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To add the supplicant MAC address `0009.41A4.5943` to force authorized port control for interface `port1.0.2`, use the following commands:

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

To delete the supplicant MAC address `0009.41A4.5943` for interface `port1.0.2`, use the following commands:

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

To reset reauthentication to disable for the supplicant MAC address `0009.41A4.5943`, for interface `port1.0.2` use the following commands:

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

Validation Commands **show dot1x**
show dot1x interface
show running-config

auth timeout connect-timeout

This command sets the connect-timeout period for the interface.

Use the **no** variant of this command to reset the connect-timeout period to the default (30 seconds).

Syntax

```
auth timeout connect-timeout <1-65535>
no auth timeout connect-timeout
```

Parameter	Description
<1-65535>	Seconds.

Default The connect-timeout default is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage This command is used for MAC- and Web-Authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When **auth-web-server session-keep** or **auth two-step enable** is enabled it is recommended to configure a longer connect-timeout period.

Examples To set the connect-timeout period to `3600` for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for interface `port1.0.2`, use the following commands:

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

Validation Commands **show dot1x**
show dot1x interface

auth timeout quiet-period

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

Use the **no** variant of this command to reset quiet period to the default (60 seconds).

Syntax

```
auth timeout quiet-period <1-65535>
no auth timeout quiet-period
```

Parameter	Description
<1-65535>	Seconds.

Default The quiet period of port authentication is 60 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the quiet period to `10` for interface `port1.0.2`, use the following commands:

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

To reset the quiet period to the default (60 seconds) for interface `port1.0.2`, use the following commands:

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

auth timeout reauth-period

This command sets the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no** variant of this command to reset the **reauth-period** parameter to the default (3600 seconds).

Syntax

```
auth timeout reauth-period <1-4294967295>
no auth timeout reauth-period
```

Parameter	Description
<1-4294967295>	Seconds.

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

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the reauthentication period to 1 day for interface `port1.0.2`, use the following commands:

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

To reset the reauthentication period to the default (3600 seconds) for interface `port1.0.2`, use the following commands:

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

Validation Commands
show dot1x
show dot1x interface
show running-config

Related Commands
auth reauthentication

auth timeout server-timeout

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

The **no** variant of this command resets the server-timeout to the default (30 seconds).

Syntax

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

Parameter	Description
<1-65535>	Seconds.

Default The server timeout for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the server timeout to 120 seconds for interface `port1.0.2`, use the following commands:

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

To set the server timeout to the default (30 seconds) for interface `port1.0.2`, use the following commands:

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

Validation Commands
show dot1x
show dot1x interface
show running-config

auth timeout supp-timeout

This command sets the timeout of the waiting response from the supplicant (client device) on a given interface.

The **no** variant of this command resets the supplicant timeout to the default (30 seconds).

Syntax

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

Parameter	Description
<1-65535>	Seconds.

Default The supplicant timeout of port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the server timeout to `2` seconds for interface `port1.0.2`, use the following commands:

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

To reset the server timeout to the default (30 seconds) for interface `port1.0.2`, use the following commands:

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

Validation Commands

show dot1x
show dot1x interface
show running-config

auth two-step enable

This command enables a two-step authentication feature on an interface. When this feature is enabled, the supplicant is authorized in a two-step process. If authentication succeeds, the supplicant becomes authenticated. This command will apply the two-step authentication method based on 802.1X-, MAC- or Web-Authentication.

The **no** variant of this command disables the two-step authentication feature.

Syntax

```
auth two-step enable
no auth two-step enable
```

Default Default.

Mode Interface Configuration for a port.

Usage The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device.

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

Examples To enable the two step authentication feature, use the following commands:

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

To disable the two step authentication feature, use the following commands:

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

To enable MAC-Authentication followed by 802.1X-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable MAC-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable 802.1X-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

Validation Commands

show startup-config
show auth-mac supplicant
show dot1x supplicant

Related Commands

show auth two-step supplicant brief
show auth-mac
show auth-mac interface
show auth-mac supplicant
show auth-web
show auth-web interface
show auth-web supplicant
show dot1x
show dot1x interface
show dot1x supplicant

auth-mac enable

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

Use the **no** variant of this command to disable MAC-based authentication on an interface.

Syntax

```
auth-mac enable
no auth-mac enable
```

Default MAC-Authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Enabling **spanning-tree edgeport** on ports after enabling MAC-based authentication avoids unnecessary re-authentication when the port state changes, which does not happen when spanning tree edgeport is enabled. Note that re-authentication is correct behavior without **spanning-tree edgeport** enabled.

Applying **switchport mode access** on ports is also good practice to set the ports to access mode with ingress filtering turned on, whenever ports for MAC-Authentication are in a VLAN.

Examples To enable MAC-Authentication on interface `port1.0.2` and enable spanning tree edgeport to avoid unnecessary re-authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac enable
awplus(config-if)# spanning-tree edgeport
awplus(config-if)# switchport mode access
```

To disable MAC-Authentication on interface `port1.0.2`, use the following commands:

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

Validation Commands
show auth-mac
show auth-mac interface
show running-config

Related Commands
aaa accounting auth-mac default
aaa authentication auth-mac
spanning-tree edgeport (RSTP and MSTP)
switchport mode access

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** variant of this command resets the authentication method used to the default method (PAP) as the RADIUS authentication method used by the MAC-Authentication.

Syntax

```
auth-mac method [eap-md5|pap]
no auth-mac method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 of authentication method.
`pap`	Enable PAP of authentication method.

Default The MAC-Authentication method is PAP.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the MAC-Authentication method to `pap` on interface `port1.0.2`, use the following commands:

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

To set the MAC-Authentication method to the default on interface `port1.0.2`, use the following commands:

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

Validation Commands

show auth-mac
show auth-mac interface
show running-config

auth-mac password

This command changes the password for MAC-based authentication.

Use the **no** variant of this command to return the password to its default.

Syntax

```
auth-mac [encrypted] password <password>
no auth-mac password
```

Parameter	Description
`auth-mac`	MAC-based authentication
`encrypted`	Specify an encrypted password
`password`	Configure the password
<password>	The new password. Passwords can be up to 64 characters in length and can contain any printable characters except ■ ? ■ " (double quotes) ■ space

Default By default, the password is the MAC address of the supplicant

Mode Global Configuration

Usage Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

- some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
- you are using two-step authentication (see **"Ensuring Authentication Methods Require Different Usernames and Passwords" on page 42.28**)

Examples To change the password to `verySecurePassword`, use the commands:

```
awplus# configure terminal
awplus(config)# auth-mac password verySecurePassword
```

Validation Command **show running-config**

Related Commands **auth two-step enable**
show auth-mac

auth-mac reauth-relearning

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

Use the **no** variant of this command to disable the auth-mac re-learning option.

Syntax

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

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

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To enable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

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

To disable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

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

Validation Commands

show auth-mac
show auth-mac interface
show running-config

auth-web enable

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

Use the **no** variant of this command to disable Web-based authentication on an interface.

Syntax

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

Default Web-Authentication is disabled by default.

Mode Interface Configuration for a static channel or a switch port.

Usage Web-based authentication cannot be enabled if DHCP snooping is enabled (**service dhcp-snooping** command on page 56.24), and vice versa. You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

Examples To enable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# auth-web enable
```

To disable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# no auth-web enable
```

Validation Commands
show auth-web
show auth-web interface
show running-config

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

auth-web forward

This command enables the Web-Authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

The **no** variant of this command disables or deletes the packet forwarding feature on the interface.

Syntax

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

Parameter	Description
<ip-address>	Enable forwarding to the destination IPv4 address.
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 Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage For more information about the *<ip-address>* parameter, and an example, see the "auth-web forward" section in the **Alliedware Plus Technical Tips and Tricks.**

Examples To enable the ARP forwarding feature on interface `port1.0.2`, use the following commands:

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

To add the TCP forwarding port 137 on interface `port1.0.2`, use the following commands:

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

To add the DNS Server IP address 192.168.1.10 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth-web forward 192.168.1.10 dns
```

To disable the ARP forwarding feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward arp
```

To delete the TCP forwarding port 137 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp 137
```

To delete the all of TCP forwarding on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp
```

Validation Commands

show auth-web
show auth-web interface
show running-config

auth-web max-auth-fail

This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than has been set to the maximum number of authentication failures then login requests are refused during the quiet period.

The **no** variant of this command resets the maximum number of authentication failures to the default (three authentication failures).

Syntax

```
auth-web max-auth-fail <0-10>
no auth-web max-auth-fail
```

Parameter	Description
<0-10>	Lock count specified.

Default The **max-auth-fail** lock counter is set to three authentication failures by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the lock count to `5` on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web max-auth-fail
```

Validation Commands **show auth-web**
show auth-web interface
show running-config

Related Commands **auth timeout quiet-period**

auth-web method

This command sets the authentication method of Web-Authentication that is used with RADIUS on the interface specified.

The **no** variant of this command sets the authentication method to PAP for the interface specified when Web-Authentication is also used with the RADIUS authentication method.

Syntax

```
auth-web method {eap-md5|pap}
no auth-web method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 as the authentication method.
`pap`	Enable PAP as the authentication method.

Default The Web-Authentication method is set to PAP by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Example To set the Web-Authentication method to eap-md5 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web method eap-md5
```

Validation Commands

show auth-web
show auth-web interface
show running-config

auth-web-server blocking-mode

Use this command to enable blocking mode for the Web-Authentication server. The blocking mode displays an authentication success or failure screen immediately from the response result from a RADIUS server.

Use the **no** variant of this command to disable blocking mode for the Web-Authentication server.

Syntax

```
auth-web-server blocking-mode

no auth-web-server blocking-mode
```

Parameter	Description
`blocking-mode`	Use blocking authentication server process.
`no`	Disable blocking mode.

Default By default, blocking mode is disabled for the Web-Authentication server.

Mode Global Configuration

Example To enable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server blocking-mode
```

To disable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server blocking-mode
```

Validation Commands **show running-config**

Related Commands **show auth-web-server**
auth-web-server mode (deleted)
auth-web-server redirect-delay-time

auth-web-server dhcp ipaddress

Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the **no** variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

Syntax

```
auth-web-server dhcp ipaddress <ip-address/prefix-length>
no auth-web-server dhcp ipaddress
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants.

Default No IP address for the Web-Authentication server is set by default.

Mode Global Configuration

Usage See the section **"DHCP server for Web-Authentication" on page 42.16** in **Chapter 42, Authentication Introduction and Configuration** for further overview information about the Web-Authentication enhancements, allowing Web-Authentication to work as seamlessly as 802.1X-Authentication.

See the section **"Limitations on Allowed Feature Combinations" on page 42.35** for information about restrictions regarding combinations of authentication enhancements working together.

Examples To assign the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

Validation Commands **show running-config**

Related Commands **show auth-web-server**
auth-web-server dhcp lease

auth-web-server dhcp lease

Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

Syntax

```
auth-web-server dhcp lease <20-60>
no auth-web-server dhcp lease
```

Parameter	Description
<20-60>	DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds.

Default The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

Mode Global Configuration

Usage See the section **"DHCP server for Web-Authentication" on page 42.16** in **Chapter 42, Authentication Introduction and Configuration** for further overview information about the Web-Authentication enhancements, allowing Web-Authentication to work as seamlessly as 802.1X-Authentication.

See the section **"Limitations on Allowed Feature Combinations" on page 42.35** for information about restrictions regarding combinations of authentication enhancements working together.

Examples To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

Validation Commands **show running-config**

Related Commands **show auth-web-server**
auth-web-server dhcp ipaddress

auth-web-server dhcp-wpad-option

This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the "Web Auth Proxy" section in the **Alliedware Plus Technical Tips and Tricks.**

Use the **no** variant of this command to disable the DHCP WPAD function.

Syntax

```
auth-web-server dhcp wpad-option <url>
no auth-web-server dhcp wpad-option
```

Parameter	Description
<url>	URL to the server which gets a .pac file.

Default The Web-Authentication server DHCP WPAD option is not set.

Mode Global Configuration

Usage If the supplicant is configured to use WPAD, the supplicant's web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

Example To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
http://192.168.1.100/proxy/
proxy.pac
```

Related Commands **show auth-web-server**

auth-web-server gateway (deleted)

This command has been deleted.

auth-web-server host-name

This command assigns a hostname to the web authentication server.

Use the **no** variant of this command to remove the hostname from the web authentication server.

Syntax

```
auth-web-server host-name <hostname>
no auth-web-server host-name
```

Parameter	Description
<hostname>	URL string of the hostname

Default The web authentication server has no hostname.

Mode Global Configuration

Usage When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

Examples To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

Related Commands **aaa authentication auth-web**
auth-web enable

auth-web-server http-redirect (deleted)

This command has been deleted.

auth-web-server intercept-port

This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the **no** variant of this command to stop intercepting the TCP port numbers.

Syntax

```
auth-web-server intercept-port <1-65535>
no auth-web-server intercept-port <1-65535>
```

Parameter	Description
<1-65535>	TCP port number.

Default No additional TCP port numbers are intercepted by default.

Mode Global Configuration

Usage If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant's initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can now use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server's network as a 'No Proxy' network. You can specify 'No Proxy' networks in the proxy settings in your web browser. For more information, see the "Web Auth Proxy" section in the **Alliedware Plus Technical Tips and Tricks.**

Example To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

Related Commands **show auth-web-server**

auth-web-server ipaddress

This command sets the IP address for the Web-Authentication server.

Use the **no** variant of this command to delete the IP address for the Web-Authentication server.

Syntax

```
auth-web-server ipaddress <ip-address>
no auth-web-server ipaddress
```

Parameter	Description
<ip-address>	Web-Authentication server dotted decimal IP address in A.B.C.D format.

Default The Web-Authentication server address on the system is not set by default.

Mode Global Configuration

Examples To set the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ipaddress
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server login-url

This command sets the web-authentication login page URL.

Use the **no** variant of this command to delete the set URL.

Syntax

```
auth-web-server login-url <URL>
no auth-web-server login-url
```

Parameter	Description
<URL>	Set login page URL

Default The built-in login page is set by default.

Mode Global Configuration

Examples To set http://example.com/login.html as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url http://
example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

Validation Commands **show running-config**

auth-web-server mode (deleted)

This command has been deleted.

auth-web-server page logo

This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

Syntax

```
auth-web-server page logo {auto|default|hidden}
no auth-web-server page logo
```

Parameter	Description
`auto`	Display the custom logo if installed; otherwise display the default logo
`default`	Display the default logo
`hidden`	Hide the logo

Default Logo type is **auto** by default.

Mode Global Configuration

Examples To display the default logo with ignoring installed custom logo, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

Validation Commands **show auth-web-server page**

auth-web-server page sub-title

This command sets the custom sub-title on the web authentication page.

Use the **no** variant of this command to reset the sub-title to its default.

Syntax

```
auth-web-server page sub-title {hidden|text <sub-title>}
no auth-web-server page sub-title
```

Parameter	Description
`hidden`	Hide the sub-title
<sub-title>	Text string of the sub-title

Default "Allied-Telesis" is displayed by default.

Mode Global Configuration

Examples To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web
Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

Validation Commands **show auth-web-server page**

auth-web-server page success-message

This command sets the success message on the web-authentication page.

Use the **no** variant of this command to remove the success message.

Syntax

```
auth-web-server page success-message text <success-message>
no auth-web-server page success-message
```

Parameter	Description
<success-message>	Text string of the success message

Default No success message is set by default.

Mode Global Configuration

Examples To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page success-message text
Your success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page success-message
```

Validation Commands **show auth-web-server page**

auth-web-server page title

This command sets the custom title on the web authentication page.

Use the **no** variant of this command to remove the custom title.

Syntax

```
auth-web-server page title {hidden|text <title>}
no auth-web-server page title
```

Parameter	Description
`hidden`	Hide the title
`<title>`	Text string of the title

Default "Web Access Authentication Gateway" is displayed by default.

Mode Global Configuration

Examples To set the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```

To hide the title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```

To unset the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

Validation Commands **show auth-web-server page**

auth-web-server page welcome-message

This command sets the welcome message on the web-authentication page.

Use the **no** variant of this command to remove the welcome message.

Syntax

```
auth-web-server page welcome-message text <welcome-message>
no auth-web-server page welcome-message
```

Parameter	Description
<welcome-message>	Text string of the welcome message

Default No welcome message is set by default.

Mode Global Configuration

Examples To set the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page welcome-message text
Your welcome message
```

To remove the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page welcome-message
```

Validation Commands **show auth-web-server page**

auth-web-server ping-poll enable

This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The **no** variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

Syntax

```
auth-web-server ping-poll enable
no auth-web-server ping-poll enable
```

Default The ping polling feature for Web-Authentication is disabled by default.

Mode Global Configuration

Examples To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server ping-poll failcount

This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

Syntax

```
auth-web-server ping-poll failcount <1-100>
no auth-web-server ping-poll failcount
```

Parameter	Description
<1-100>	Count.

Default The default failcount for ping polling is 5 pings.

Mode Global Configuration

Examples To set the failcount of ping polling to `10` pings, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

Validation Commands

show auth-web
show auth-web-server
show running-config

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 (client device) is reachable.

Use the **no** variant of this command to reset to the default period for ping polling (30 seconds).

Syntax

```
auth-web-server ping-poll interval <1-65535>
no auth-web-server ping-poll interval
```

Parameter	Description
<1-65535>	Seconds.

Default The interval for ping polling is 30 seconds by default.

Mode Global Configuration

Examples To set the interval of ping polling to `60` seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll interval
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server ping-poll reauth-timer-refresh

This command modifies the **reauth-timer-refresh** parameter for the Web-Authentication feature. The **reauth-timer-refresh** parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the **no** variant of this command to reset the **reauth-timer-refresh** parameter to the default setting (disabled).

Syntax

```
auth-web-server ping-poll reauth-timer-refresh
no auth-web-server ping-poll reauth-timer-refresh
```

Default The `reauth-timer-refresh` parameter is disabled by default.

Mode Global Configuration

Examples To enable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll reauth-timer-refresh
```

To disable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll reauth-timer-
refresh
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server ping-poll timeout

This command modifies the ping poll **timeout** parameter for the Web-Authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

Syntax

```
auth-web-server ping-poll timeout <1-30>
no auth-web-server ping-poll timeout
```

Parameter	Description
<1-30>	Seconds.

Default The default timeout for ping polling is 1 second.

Mode Global Configuration

Examples To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server port

This command sets the HTTP port number for the Web-Authentication server.

Use the **no** variant of this command to reset the HTTP port number to the default (80).

Syntax

```
auth-web-server port <port-number>
no auth-web-server port
```

Parameter	Description
<port-number>	Set the local Web-Authentication server port within the TCP port number range 1 to 65535.

Default The Web-Authentication server HTTP port number is set to 80 by default.

Mode Global Configuration

Examples To set the HTTP port number `8080` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number `80` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server redirect-delay-time

Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant **no** to reset the delay time set previously.

Syntax

```
auth-web-server redirect-delay-time <5-60>
no auth-web-server redirect-delay-time
```

Parameter	Description
`redirect-delay-time`	Set the delay time before jumping to a specified URL after the supplicant is authorized.
<5-60>	The time in seconds.

Default The default redirect delay time is `5` seconds.

Mode Global Configuration

Examples To set the delay time to `60` seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

Validation Command **show auth-web-server**
show running-config

Related Commands **auth-web-server redirect-url**
show auth-web-server

auth-web-server redirect-url

This command sets a URL for supplicant (client device) authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no** variant of this command to delete the URL string set previously.

Syntax

```
auth-web-server redirect-url <url>
no auth-web-server redirect-url
```

Parameter	Description
<url>	URL (hostname or dotted IP notation).

Default The redirect URL for the Web-Authentication server feature is not set by default (null).

Mode Global Configuration

Examples To enable and set redirect a URL string `www.alliedtelesis.com` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url
                http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

Validation Commands
show auth-web
show auth-web-server
show running-config

Related Commands
auth-web-server http-redirect (deleted)
auth-web-server redirect-delay-time

auth-web-server session-keep

This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentication.

Use the **no** variant of this command to disable the session keep feature.

Syntax

```
auth-web-server session-keep
no auth-web-server session-keep
```

Default The session-keep feature is disabled by default.

Mode Global Configuration

Usage This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

Examples To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server ssl

This command enables HTTPS functionality for the Web-Authentication server feature.

Use the **no** variant of this command to disable HTTPS functionality for the Web-Authentication server.

Syntax

```
auth-web-server ssl
no auth-web-server ssl
```

Default HTTPS functionality for the Web-Authentication server feature is disabled by default.

Mode Global Configuration

Examples To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl
```

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl
```

Validation Commands

show auth-web
show auth-web-server
show running-config

auth-web-server sslport (deleted)

This command has been deleted.

auth-web-server ssl intercept-port

Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the **auth-web-server intercept-port** command to register HTTP intercept port numbers.

Use the **no** variant of this command to delete registered port number.

Syntax

```
auth-web-server ssl intercept-port <1-65535>
no auth-web-server ssl intercept-port <1-65535>
```

Parameter	Description
<1-65535>	TCP port number in the range from 1 through 65535

Default 443/TCP is registered by default.

Mode Global Configuration

Examples To register HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

Validation Commands **show auth-web-server**

Related Commands **auth-web-server intercept-port**

copy proxy-autoconfig-file

Use this command to download the proxy auto configuration (PAC) file to your switch. The Web-Authentication supplicant can get the downloaded file from the system web server.

Syntax `copy <filename> proxy-autoconfig-file`

Parameter	Description
<filename>	The URL of the PAC file.

Mode Privileged Exec

Example To download the PAC file to this device, use the command:

```
awplus# copy tftp://server/proxy.pac proxy-autoconfig-file
```

Related Commands **show proxy-autoconfig-file**
erase proxy-autoconfig-file

copy web-auth-https-file

Use this command to download the SSL server certificate for web-based authentication. The file must be in PEM (Privacy Enhanced Mail) format, and contain the private key and the server certificate.

Syntax `copy <filename> web-auth-https-file`

Parameter	Description
<filename>	The URL of the server certificate file.

Mode Privileged Exec

Example To download the server certificate file `veriSign_cert.pem` from the TFTP server directory `server`, use the command:

```
awplus# copy tftp://server/veriSign_cert.pem web-auth-https-
       file
```

Related Commands **auth-web-server ssl**
erase web-auth-https-file
show auth-web-server

erase proxy-autoconfig-file

Use this command to remove the proxy auto configuration file.

Syntax `erase proxy-autoconfig-file`

Mode Privileged Exec

Example To remove the proxy auto configuration file, use the command:

```
awplus# erase proxy-autoconfig-file
```

Related Commands **show proxy-autoconfig-file**
copy proxy-autoconfig-file

erase web-auth-https-file

Use this command to remove the SSL server certificate for web-based authentication.

Syntax `erase web-auth-https-file`

Mode Privileged Exec

Example To remove the SSL server certificate file for web-based authentication use the command:

```
awplus# erase web-auth-https-file
```

Related Commands **auth-web-server ssl**
copy web-auth-https-file
show auth-web-server

show auth two-step supplicant brief

This command displays the supplicant state of the two-step authentication feature on the interface.

Syntax `show auth two-step supplicant [interface <ifrange>] brief`

Parameter	Description
`interface`	The interface selected for display.
<ifrange>	The interface which can be specified as *<ifrange>* - Switch port (e.g. port1.0.12) - Static channel group (e.g. sa3) - Dynamic (LACP) channel group (e.g. po4)

Mode Privileged Exec

Usage Do not mix interface types in a list. The specified interfaces must exist.

Example To display the supplicant state of the two-step authentication feature, enter the command:

```
awplus# show two-step supplicant interface
        port1.0.12 brief
```

Output **Figure 43-1: Example output from the show auth two-step supplicant brief command**

```
interface port1.0.12
  authenticationMethod: dot1x/mac
  Two-Step Authentication:
    firstMethod:mac
    secondMethod:dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

Interface  VID Mode  MAC Address       Status          FirstStep     SecondStep
========== === ====  ===========       ======          =========     ==========
port1.0.12   1   D    000b..db67.00f7   Authenticated   Pass          Pass
```

Related Commands **auth two-step enable**

show auth-mac

This command shows authentication information for MAC-based authentication.

Syntax `show auth-mac [all]`

Parameter	Description
`all`	Display all authentication information for each interface available on the switch.

Mode Privileged Exec

Example To display all MAC-based authentication information, enter the command:

```
awplus# show auth-mac all
```

Output **Figure 43-2: Example output from the show auth-mac command**

```
802.1X Port-Based Authentication Disabled
MAC-based Port Authentication Enabled
WEB-based Port Authentication Disabled
```

Related Commands **show dot1x**
show auth-web

show auth-mac diagnostics

This command shows MAC-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax `show auth-mac diagnostics [interface <interface-list>]`

Parameter	Description
`interface`	Specify an interface to show
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication diagnostics for `port1.0.6`, enter the command:

```
awplus# show auth-mac diagnostics interface port1.0.6
```

Output **Figure 43-3: Example output from the show auth-mac diagnostics command**

```
Authentication Diagnostics for interface port1.0.6
    Supplicant address: 00d0.59ab.7037
        authEnterConnecting: 2
        authEaplogoffWhileConnecting: 1
        authEnterAuthenticating: 2
        authSuccessWhileAuthenticating: 1
        authTimeoutWhileAuthenticating: 1
        authFailWhileAuthenticating: 0
        authEapstartWhileAuthenticating: 0
        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, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

Syntax

```
show auth-mac interface <interface-list> [diagnostics|
   sessionstatistics|statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session statistics.
`statistics`	Statistics.
`supplicant`	Supplicant (client device).
`brief`	Brief summary of supplicant state.

Mode Privileged Exec

Examples To display MAC-based authentication status for `port1.0.2`, enter the command:

```
awplus# show auth-mac interface port1.0.2
```

```
% Port-Control not configured on port1.0.2
```

To display MAC-Authentication diagnostics for `port1.0.2`, enter the command:

```
awplus# show auth-mac interface port1.0.2 diagnostics
```

```
Authentication Diagnostics for interface port1.0.2
    Supplicant address: 00d0.59ab.7037
        authEnterConnecting: 2
        authEaplogoffWhileConnecting: 1
        authEnterAuthenticating: 2
        authSuccessWhileAuthenticating: 1
        authTimeoutWhileAuthenticating: 1
        authFailWhileAuthenticating: 0
        authEapstartWhileAuthenticating: 0
        authEaplogoggWhileAuthenticating: 0
        authReauthsWhileAuthenticated: 0
        authEapstartWhileAuthenticated: 0
        authEaplogoffWhileAuthenticated: 0
        BackendResponses: 2
        BackendAccessChallenges: 1
        BackendOtherrequestToSupplicant: 3
        BackendAuthSuccess: 1
```

To display authentication session statistics for `port1.0.6`, enter the command:

```
awplus# show auth-mac interface port1.0.6 sessionstatistics
```

```
Authentication session statistics for interface port1.0.6
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

To display MAC-Authentication statistics for `port1.0.6` enter the command:

```
awplus# show auth-mac interface port1.0.6 statistics
```

To display the MAC authenticated supplicant on interface `port1.0.6`, enter the command:

```
awplus# show auth-mac interface port1.0.6 supplicant
```

Related Commands

show auth-web diagnostics
show dot1x sessionstatistics
show dot1x statistics interface
show dot1x supplicant interface

show auth-mac sessionstatistics

This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax `show auth-mac sessionstatistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify an interface to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display output displaying MAC-Authentication session statistics for `port1.0.2`, enter the command:

```
awplus# show auth-mac sessionstatistics interface port1.0.2
```

Output **Figure 43-4: Example output from the show auth-mac sessionstatistics command**

```
Authentication session statistics for interface port1.0.2
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

show auth-mac statistics interface

This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax `show auth-mac statistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify ports to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display MAC-Authentication statistics for `port1.0.2`, enter the command:

```
awplus# show auth-mac statistics interface port1.0.2
```

Related Commands **show dot1x interface**

show auth-mac supplicant

This command shows the supplicant (client device) state when MAC-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-mac supplicant [<macadd>] [brief]`

Parameter	Description
<macadd>	Mac (hardware) address of the Supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Example To display the MAC authenticated supplicant for MAC address `00d0.59ab.7037`, enter the command:

```
awplus# show auth-mac supplicant 00d0.59ab.7037
```

```
Web authentication server
    Server status: enabled
    Server address: -
    HTTP Port No: 80
    Security: enabled
    Certification: default
    SSL Port No: 443
    Redirect URL:
    Redirect Delay Time: 30
    HTTP Redirect: disabled
    Session keep: disabled
    PingPolling: disable
    PingInterval: 30
    Timeout: 1
    FailCount: 5
    ReauthFresh: disabled
```

Example To display a brief summary output for a MAC authenticated supplicant, enter the command:

```
awplus# show auth-mac supplicant brief
```

For example, if two-step authentication is configured with MAC-Authentication as the first method and 802.1X-Authentication as the second method then the output is as follows:

```
Interface port1.0.6
  authenticationMethod: dot1x/mac
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= ==============  =========
port1.0.6   5    D    0008.0d5e.c216 Authenticated     --              dot1x
```

For example, if two-step authentication is configured with MAC-Authentication as the first method and Web-Authentication as the second method then the output is as follows:

```
Interface port1.0.7
  authenticationMethod: mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== =========
port1.0.7   5    W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

show auth-mac supplicant interface

This command shows the supplicant (client device) state for the MAC authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-mac supplicant [interface <interface-list>] [brief]`

Parameter	Description
`interface`	Specify ports to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display the MAC authenticated supplicant on the interface `port1.0.2`, enter the command:

```
awplus# show auth-mac supplicant interface port1.0.2
```

show auth-web

This command shows authentication information for Web-based authentication.

Syntax `show auth-web [all]`

Parameter	Description
`all`	Display all authentication information for each authenticated interface. This can be a static channel (or static aggregator), or a dynamic (or LACP) channel group, or a switch port.

Mode Privileged Exec

Example To display all Web-Authentication information, enter the command:

```
awplus# show auth-web all
```

Output **Figure 43-5: Example output from the show auth-web command**

```
awplus# show auth-web all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
 RADIUS server address (auth): 150.87.17.192:1812
   Last radius message id: 4
Authentication Info for interface port1.0.1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
 twoStepAuthentication:
   configured: enabled
   actual: enabled
 supplicantMac: none
 Supplicant name: oha
 Supplicant address: 000d.6013.5398
   authenticationMethod: WEB-based Authentication
   Two-Step Authentication:
     firstAuthentication: Pass - Method: dot1x
     secondAuthentication: Pass - Method: web
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

Related Commands **show dot1x**
show auth-mac

show auth-web diagnostics

This command shows Web-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax `show auth-web diagnostics [interface <interface-list>]`

Parameter	Description
`interface`	Specify ports to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication diagnostics for `port1.0.6`, enter the command:

```
awplus# show auth-web diagnostics interface port1.0.6
```

Output **Figure 43-6: Example output from the show auth-web diagnostics command**

```
Authentication Diagnostics for interface port1.0.6
    Supplicant address: 00d0.59ab.7037
        authEnterConnecting: 2
        authEaplogoffWhileConnecting: 1
        authEnterAuthenticating: 2
        authSuccessWhileAuthenticating: 1
        authTimeoutWhileAuthenticating: 1
        authFailWhileAuthenticating: 0
        authEapstartWhileAuthenticating: 0
        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, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

Syntax

```
show auth-web interface <interface-list> [diagnostics|
   sessionstatistics|statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session statistics.
`statistics`	Statistics.
`supplicant`	Supplicant (client device).
`brief`	Brief summary of supplicant state.

Mode Privileged Exec

Example To display the Web based authentication status for `port1.0.6`, enter the command:

```
awplus# show auth-web interface port1.0.6
```

To display the Web based authentication status for `port1.0.1`, enter the command:

```
awplus# show auth-web interface port1.0.1
```

```
awplus# show auth-web interface port1.0.1
Authentication Info for interface port1.0.1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
 twoStepAuthentication:
   configured: enabled
   actual: enabled
 supplicantMac: none
```

To display Web-Authentication diagnostics for `port1.0.6`, enter the command:

```
awplus# show auth-web interface port1.0.6 diagnostics
```

```
Authentication Diagnostics for interface port1.0.6
    Supplicant address: 00d0.59ab.7037
        authEnterConnecting: 2
        authEaplogoffWhileConnecting: 1
        authEnterAuthenticating: 2
        authSuccessWhileAuthenticating: 1
        authTimeoutWhileAuthenticating: 1
        authFailWhileAuthenticating: 0
        authEapstartWhileAuthenticating: 0
        authEaplogoggWhileAuthenticating: 0
        authReauthsWhileAuthenticated: 0
        authEapstartWhileAuthenticated: 0
        authEaplogoffWhileAuthenticated: 0
        BackendResponses: 2
        BackendAccessChallenges: 1
        BackendOtherrequestToSupplicant: 3
        BackendAuthSuccess: 1
```

To display Web-Authentication session statistics for `port1.0.6`, enter the command:

```
awplus# show auth-web interface port1.0.6 sessionstatistics
```

```
Authentication session statistics for interface port1.0.6
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

To display Web-Authentication statistics for `port1.0.6`, enter the command:

```
awplus# show auth-web statistics interface port1.0.6
```

To display the Web-Authenticated supplicant on interface `port1.0.6`, enter the command:

```
awplus# show auth-web interface port1.0.6 supplicant
```

Related Commands

show auth-web diagnostics
show dot1x sessionstatistics
show dot1x statistics interface
show dot1x supplicant interface

show auth-web sessionstatistics

This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax `show auth-web sessionstatistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify ports to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication statistics for `port1.0.6`, enter the command:

```
awplus# show auth-web sessionstatistics interface port1.0.6
```

Output **Figure 43-7: Example output from the show auth-web sessionstatistics command**

```
Authentication session statistics for interface port1.0.6
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

show auth-web statistics interface

This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax `show auth-web statistics interface <interface-list>`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display Web-Authentication statistics for `port1.0.4`, enter the command:

```
awplus# show dot1x statistics interface port1.0.4
```

Related Commands **show dot1x interface**

show auth-web supplicant

This command shows the supplicant (client device) state when Web-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-web supplicant [<macadd>] [brief]`

Parameter	Description
`<macadd>`	Mac (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display Web authenticated supplicant information on the switch, enter the command:

```
awplus# show auth-web supplicant
```

show auth-web supplicant interface

This command shows the supplicant (client device) state for the Web authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional **brief** parameter is used.

Syntax `show auth-web supplicant interface <interface-list> [brief]`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display the Web authenticated supplicant on the interface `port1.0.3`, enter the command:

```
awplus# show auth-web supplicant interface port1.0.3
```

To display brief summary output for the Web authenticated supplicant, enter the command:

```
awplus# show auth-web supplicant brief
```

show auth-web-server

This command shows the Web-Authentication server configuration and status on the switch.

Syntax `show auth-web-server`

Mode Privileged Exec

Example To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

Output **Figure 43-8: Example output from the show auth-web-server command**

```
Web authentication server
    Server status: enabled
    Server mode: none
    Server address: 192.168.1.1/24
      DHCP server enabled
      DHCP lease time: 20
      DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
    HTTP Port No: 80
    Security: disabled
    Certification: default
    SSL Port No: 443
    Redirect URL: --
    Redirect Delay Time: 5
    HTTP Redirect: enabled
    Session keep: disabled
    PingPolling: disabled
    PingInterval: 30
    Timeout: 1
    FailCount: 5
    ReauthTimerReFresh: disabled
```

Related Commands
auth-web-server gateway (deleted)
auth-web-server http-redirect (deleted)
auth-web-server ipaddress
auth-web-server port
auth-web-server redirect-delay-time
auth-web-server redirect-url
auth-web-server session-keep
auth-web-server ssl
auth-web-server sslport (deleted)

show auth-web-server page

his command displays the web-authentication page configuration and status.

Syntax `show auth-web-server page`

Mode Privileged Exec

Examples To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Figure 44: Example output from the show auth-web-server page command on the console.

```
awplus#show auth-web-server page
Web authentication page
  Logo: auto
  Title: default
  Sub-Title: Web Authentication
  Welcome message: Your welcome message
  Success message: Your success message
```

Related Commands
auth-web forward
auth-web-server page logo
auth-web-server page sub-title
auth-web-server page success-message
auth-web-server page title
auth-web-server page welcome-message

show proxy-autoconfig-file

This command displays the contents of the proxy auto configuration (PAC) file.

Syntax `show proxy-autoconfig-file`

Mode Privileged Exec

Example To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

Output **Figure 43-9: Example output from the show proxy-autoconfig-file**

```
function FindProxyForURL(url,host)
{
 if (isPlainHostName(host) ||
     isInNet(host, "192.168.1.0","255.255.255.0")) {
   return "DIRECT";
}
 else {
   return "PROXY 192.168.110.1:8080";
 }
}
```

Related Commands copy proxy-autoconfig-file
erase proxy-autoconfig-file

Chapter 44: AAA Introduction and Configuration

AAA Introduction 44.2
Available Functions and Server Types 44.2
Server Groups and Method Lists 44.3
Configuring AAA Login Authentication 44.5
AAA Configuration Tasks 44.5
Sample Authentication Configurations 44.7
Sample 802.1X-Authentication Configuration 44.7
Sample MAC-Authentication Configuration 44.8
Sample Web-Authentication Configuration 44.9
Sample Tri-Authentication Configuration 44.10

AAA Introduction

AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These function can be applied in a variety of methods with a variety of servers. The purpose of the AAA commands is to map instances of the AAA functions to sets of servers.

The Authentication function can be performed in multiple contexts, such as authentication of users logging in at a console, or 802.1X-Authentication of devices connecting to Ethernet ports.

For each of these contexts, you may want to use different sets of servers for examining the proffered authentication credentials and deciding if they are valid. AAA Authentication commands enable you to specify which servers will be used for different types of authentication.

Available Functions and Server Types

Authentication, Authorization and Accounting functions are available.

Authentication is performed in the following contexts:

- Login authentication of user shell sessions on the console port, and via telnet/SSH
- Enable password authentication for user shell sessions on the console port, and via telnet/SSH (TACACS+ only)
- 802.1X-Authentication of devices connecting to switch ports
- MAC-Authentication of devices connecting to switch ports
- Web-based authentication of devices connecting to switch ports

Authorization is performed in the following context:

- TACACS+ login authentication. Note that with the AlliedWare Plus TACACS+ implementation:
  - « authorization cannot be performed independently of the login authentication process
  - « authorization will not be attempted if enable password authentication is configured
  - « there are no authorization commands available

Accounting is performed in the following contexts:

- Accounting of console, telnet, and SSH login sessions
- Accounting of commands executed within user shell sessions (TACACS+ only)
- Accounting of 802.1X-Authenticated connections
- Accounting of MAC-Authenticated connections
- Accounting of Web-Authenticated connections

The three types of servers that can be used are:

- Local user database
- RADIUS servers
- TACACS+ servers

Server Groups and Method Lists

There are two constructs that underlie the structure of the AAA commands:

- Server groups are lists of RADIUS servers
- Method Lists are lists of server types

Server groups

A server group is defined by the command **aaa group server**. This command puts you into Server Group configuration mode.

Any number of servers can be added to a group. Typically, you will add servers which have already been configured by the command **radius-server host**. If you add a server that has not yet been configured by the command **radius-server host**, you will receive a warning that the server has not yet been configured, but the command will be accepted.

There is one server group that is always present on the switch by default that cannot be removed. It is the group simply named **radius** that comprises all servers that have been configured using the command **radius-server host**. As soon as a server is configured by the command **radius-server host**, it is automatically a member of the server group **radius** and cannot be removed from it.

Method lists

A method list defines the set of server types that you want to be used for authenticating a user/device, and the order in which you want the server types to be used.

- You may want the usernames proffered for logging in at the console to be checked for in the local user database. You can create a server list that specifies **local**.
- You may want to check the TACACS+ servers first, and resort to the local user database if none of the TACACS+ servers respond. You can create a server list that specifies **group tacacs+** first, followed by **local**.
- You may want to check the RADIUS servers first, and resort to the local user database if none of the RADIUS servers respond. You can create a server list that specifies **group radius** first, followed by **local**.

A method list defines the servers where authentication requests are sent. The first server listed is used to authenticate users; if that server fails then the next authentication server type in the method list is selected. This process continues until there is a successful authentication or until all server types fail.

When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies `group tacacs+ local`, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers not the local user database; the user login fails.

Default method lists

For every authentication or accounting type, it is always possible to define a method list called **default**. For most of the authentication and accounting types, the only method list that can be defined is default.

As soon as the default method list is defined for a given authentication or accounting type, it is automatically applied as the method list to be used for any instance of that type of authentication or accounting, except for instances to which another named method list has been specifically applied.

Configuring AAA Login Authentication

To configure AAA authentication, create default or a named method list for different authentication types. In the case of login authentication, the named method lists are then applied to consoles or VTY lines.

AAA Configuration Tasks

To define how a given accounting or authentication type will be applied to a given port or line:

- either create a server group using the **aaa group server** command (RADIUS only),
- or create a method list for the authentication or accounting type as required,
- then apply that method list to the port or line as required.

Step 1: Define a group of RADIUS servers

Create a server group using the **aaa group server** command.

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
```

Step 2: Specify the login authentication or accounting method list

Create a method list for the authentication (**aaa authentication login**) or accounting (**aaa accounting login**) type as required.

To configure a user login authentication method list called `USERS` to use first all available RADIUS servers for user login authentication and then the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
radius
```

To configure a user login authentication method list called `USERS` to use first the TACACS+ servers for user login authentication and then the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

Step 3: Apply method list to interface port or line

Apply that method list to the port or line as required.

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# login authentication USERS
```

For most Authentication and Accounting types, the only possible server list is **default**, and the only server that can be put into it is **radius**. You will typically use all RADIUS servers, so **group radius** can be used, rather than having to create a specific user group. Often the configuration of a given Authentication or Accounting type will consist of a single command, the command that defines the default server list, which contains just one server.

AAA 802.1X-Authentication configuration

AAA 802.1X-Authentication will typically be configured with the following commands.

To enable 802.1X-Authentication globally for all RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x default group radius
```

Sample Authentication Configurations

Sample 802.1X-Authentication Configuration

See the below sample configuration script for a sample 802.1X-Authentication configuration. Copy and paste then edit the sample 802.1X-Authentication configuration in your config file. See the **edit** command in the **Chapter 7, File Management Commands** for further information.

Output

Figure 44-1: Sample 802.1X-Authentication configuration

```
!
 radius-server host 192.168.1.2 key secret-key-radius-server
!
 aaa authentication dot1x default group radius
!
 no spanning-tree rstp enable
!
 interface port1.0.1
 switchport
 switchport mode access
 dot1x port-control auto
!
 interface vlan1
 ip address 192.168.1.120/24
!
```

The 802.1X-Authentication feature needs the **aaa authentication dot1x** command and the **dot1x port-control** command configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 47, 802.1X Commands** for command information to edit this configuration.

This sample configuration enables 802.1X-Authentication on interface `vlan1` with IP address `192.168.1.120`. Change the VLAN ID and IP address as required for your configuration.

Sample MAC-Authentication Configuration

See the below sample configuration script for a sample MAC-Authentication configuration. Copy, paste, and edit the sample MAC-Authentication configuration in the config file.

See the **edit** command in the **Chapter 7, File Management Commands** for further information.

Output

Figure 44-2: Sample MAC-Authentication configuration

```
!
 radius-server host 192.168.1.2 key secret-key-radius-server
!
 aaa authentication auth-mac default group radius
!
 no spanning-tree rstp enable
!
 interface port1.0.1
 switchport
 switchport mode access
 auth-mac enable
!
 interface vlan1
 ip address 192.168.1.120/24
!
```

The MAC-Authentication feature needs the **aaa authentication auth-mac** and the **auth-mac enable** commands configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 43, Authentication Commands** for command information to edit this configuration.

This configuration enables MAC-Authentication on `vlan1` with IP address `192.168.1.120`. Change the interface VLAN ID, MAC, and IP addresses as needed in your configuration.

Sample Web-Authentication Configuration

See the below sample configuration script for a sample Web-Authentication configuration. Copy, paste, and edit the sample Web-Authentication configuration for your config file.

See the **edit** command in the **Chapter 7, File Management Commands** for further information.

Output

Figure 44-3: Sample Web-Authentication configuration

```
!
 radius-server host 192.168.1.2 key secret-key-radius-server
!
 aaa authentication auth-web default group radius
!
 no spanning-tree rstp enable
!
 interface port1.0.1
 switchport
 switchport mode access
 auth-web enable
!
 interface vlan1
 ip address 192.168.1.120/24
!
```

The Web-Authentication feature needs the **aaa authentication auth-web** and the **auth-web enable** commands configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 43, Authentication Commands** for command information to edit this configuration.

The above sample Web-Authentication configuration requires the user name '`guest`' with password '`guest!`' on IP address `192.168.1.120` from interface `port1.0.1`.

Sample Tri-Authentication Configuration

See the below sample configuration script for a sample tri-authentication configuration that configures 802.1X-Authentication, MAC-Authentication, and Web-Authentication on the same interface. Copy, paste, and edit the sample tri-authentication configuration for your config file. See the **edit** command in the **Chapter 7, File Management Commands** for further information.

Output

Figure 44-4: Sample tri-authentication configuration

```
!
 radius-server host 192.168.1.2 key secret-key-radius-server
!
 aaa authentication dot1x default group radius
 aaa authentication auth-mac default group radius
 aaa authentication auth-web default group radius
!
 no spanning-tree rstp enable
!
 interface port1.0.1
 switchport
 switchport mode access
 dot1x port-control auto
 auth-mac enable
 auth-web enable
!
 interface vlan1
 ip address 192.168.1.120/24
!
```

The 802.1X-Authentication feature needs the **aaa authentication dot1x** command and the **dot1x port-control** command configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 47, 802.1X Commands** for command information to edit this configuration.

The MAC-Authentication feature needs the **aaa authentication auth-mac** and the **auth-mac enable** commands configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 43, Authentication Commands** for command information to edit this configuration.

The Web-Authentication feature needs the **aaa authentication auth-web** and the **auth-web enable** commands configured on an interface. See **Chapter 45, AAA Commands** and **Chapter 43, Authentication Commands** for command information to edit this configuration.

This sample tri-authentication configuration requires a user name '`guest`' with password '`guest!`' on IP address `192.168.1.120` from `port1.0.1`. Note this sample also configures 802.1X- and MAC-Authentication on `vlan1` with IP address `192.168.1.120`. Change the interface VLAN ID, MAC and IP address as needed for your configuration.

Note that when tri-authentication is applied to the same interface then the order of execution is MAC-Authentication first, then 802.1X- or Web-Authentication, if MAC-Authentication fails.

Chapter 45: AAA Commands

Command List 45.2
aaa accounting auth-mac default 45.2
aaa accounting auth-web default 45.4
aaa accounting wireless 45.6
aaa accounting commands 45.8
aaa accounting dot1x 45.10
aaa accounting login 45.12
aaa accounting update 45.14
aaa authentication auth-mac 45.15
aaa authentication auth-web 45.16
aaa authentication dot1x 45.17
aaa authentication enable default group tacacs+ 45.18
aaa authentication enable default local 45.20
aaa authentication login 45.21
aaa group server 45.24
aaa local authentication attempts lockout-time 45.25
aaa local authentication attempts max-fail 45.26
accounting login 45.27
clear aaa local user lockout 45.28
debug aaa 45.29
login authentication 45.30
show aaa local user locked 45.31
show debugging aaa 45.32
undebug aaa 45.32

Command List

This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see **Chapter 44, AAA Introduction and Configuration**.

aaa accounting auth-mac default

This command configures a default accounting method list for MAC-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with MAC-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for MAC-based Authentication globally.

Syntax

```
aaa accounting auth-mac default {start-stop|stop-only|none}
   group {<group-name>|radius}

no aaa accounting auth-mac default
```

Parameter	Description
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers

Default RADIUS accounting for MAC-based Authentication is disabled by default

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Use the no variant of this command to disable AAA accounting for MAC-based Authentication globally.

Examples To enable RADIUS accounting for MAC-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac default start-stop
group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac default
```

Related Commands **aaa authentication auth-mac**

aaa accounting auth-web default

This command configures a default accounting method list for Web-based Port Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with Web-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for Web-based Port Authentication globally.

Syntax

```
aaa accounting auth-web default {start-stop|stop-only|none}
    group {<group-name>|radius}

no aaa accounting auth-web default
```

Parameter	Description
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for Web-based Port Authentication is disabled by default.

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command

Configure the accounting event to be sent to the RADIUS server with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples To enable RADIUS accounting for Web-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web default start-stop
                group radius
```

To disable RADIUS accounting for Web-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web default
```

Related Commands **aaa authentication auth-web**

aaa accounting wireless

This command configures a default accounting method list for wireless clients under APs managed by Wireless Manager. The default accounting method list specifies what type of accounting messages are sent and which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to Wireless Manager.

There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius**: use a RADIUS server configured by the command **"radius-server host" on page 49.6**.
- **group <group-name>**: use the specified RADIUS server group

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.
- **none**: disables accounting.

The no variant of this command disables RADIUS accounting for wireless clients globally.

Note You can only configure one accounting server for a wireless client. If an accounting server is currently configured, you must first use the no form of the command to remove it from the configuration. The specified group can only contain one server.

Syntax

```
aaa accounting wireless default (start-stop | none) group {radius |
    <group-name>}

no aaa accounting wireless default
```

Parameter	Description
`default`	The default accounting method list
`start-stop`	Start and stop records are to be sent
`none`	No accounting records are to be sent
`group`	Use a server group
`radius`	Use a RADIUS server configured by the radius-server host command
<group-name>	The server group name

Default This command is disabled by default.

Example To enable RADIUS accounting for wireless clients under APs managed by Wireless Manager, and use an available RADIUS Server, use the commands:

```
awplus# configure terminal

awplus(config)# aaa accounting wireless default
                start-stop group radius
```

To disable RADIUS accounting for wireless clients under APs managed by Wireless Manager, use the commands:

```
awplus# configure terminal

awplus(config)# no aaa accounting wireless
default
```

Related Commands

aaa accounting wireless
aaa group server
radius-server host

aaa accounting commands

Use this command to configure and enable TACACS+ command accounting. When command accounting is enabled, information about a command entered at a specified privilege level on a device is sent to a TACACS+ server. To account for all commands entered on a device you need to configure command accounting for each discrete privilege level. A command accounting record includes the command as entered for the specified privilege level, the date and time each command execution finished, and the username of the user who executed the command.

This command creates a default method list that is applied to every console and vty line. The **stop-only** parameter indicates that an accounting message is sent to the TACACS+ server when a command has stopped executing.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured and only the first reachable server is used. If no server is found the accounting message is dropped.

Use the **no** variant of this command to disable command accounting.

Syntax

```
aaa accounting commands <1-15> default stop-only group tacacs+
no aaa accounting commands <1-15> default
```

Parameter	Description
<1-15>	The privilege level, in the range 1 to 15.

Default TACACS+ command accounting is disabled by default.

Mode Global Configuration

Usage When command accounting is enabled, the command as entered is included in the accounting packets sent to the TACACS+ accounting server.

You cannot enable command accounting if a trigger is configured. An error message is displayed if you attempt to enable command accounting and a trigger is configured.

The **show tech-support** command runs a number of commands and each command is accounted separately.

When the **copy <*filename*> running-config** command is executed all the commands of a configuration file copied into the running-config are accounted separately.

Examples To configure command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 15 default
```

Related Commands

aaa authentication login
aaa accounting login
accounting login
tacacs-server host

aaa accounting dot1x

This command configures the default accounting method list for IEEE 802.1X-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with IEEE 802.1X-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for 802.1X-based Port Authentication globally.

Syntax

```
aaa accounting dot1x default {start-stop|stop-only|none}
    group {<group-name>|radius}

no aaa accounting dot1x default
```

Parameter	Description
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
<group-name>	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for 802.1X-based Port Authentication is disabled by default (there is no default server set by default).

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command.
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples To enable RADIUS accounting for 802.1X-based Authentication, and use all available RADIUS Servers, use the commands:

```
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 and TACACS+ accounting for login shell sessions. The specified method list name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, then this creates a default method list that is applied to every console and vty line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to remove an accounting method list for login shell sessions configured by an **aaa accounting login** command. If the method list being deleted is already applied to a console or vty line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

Syntax

```
aaa accounting login {default|<list-name>}{start-stop|stop-only|none}
    {group {radius|tacacs+|<group-name>}}

no aaa accounting login {default|<list-name>}
```

Parameter	Description
`default`	Default accounting method list.
`<list-name>`	Named accounting method list.
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`group`	Specify the servers or server group where accounting packets are sent.
`radius`	Use all RADIUS servers configured by the **radius-server host** command on page 49.6.
`tacacs+`	Use all TACACS+ servers configured by the **tacacs-server host** command.
`<group-name>`	Use the specified RADIUS server group, as configured by the **aaa group server** command.

Default Accounting for login shell sessions is disabled by default.

Mode Global Configuration

Usage This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name `default` and any number of other named method lists. The *<list-name>* for any method list that you define can then be used as the *<list-name>* parameter in the **accounting login** command available from Line Configuration mode.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+** : use all TACACS+ servers configured by **tacacs-server host** command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)#  no aaa accounting login default
```

Related Commands
aaa accounting commands
aaa authentication login
aaa accounting login
aaa accounting update
accounting login
radius-server host
tacacs-server host

aaa accounting update

This command enables periodic accounting reporting to either the RADIUS or TACACS+ accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

Syntax

```
aaa accounting update [periodic <1-65535>]
no aaa accounting update
```

Parameter	Description
`periodic`	Send accounting records periodically.
<1-65535>	The interval to send accounting updates (in minutes). The default is 30 minutes.

Default Periodic accounting update is disabled by default.

Mode Global Configuration

Usage Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is reenabled, unless this interval is specified.

Examples To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting update wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting update
```

Related Commands
aaa accounting auth-mac default
aaa accounting auth-web default
aaa accounting dot1x
aaa accounting login

aaa authentication auth-mac

This command enables MAC-based Port Authentication globally and allows you to specify an authentication method list. It is automatically applied to every interface running MAC-based Port Authentication.

Use the **no** variant of this command to globally disable MAC-based Port Authentication.

Syntax

```
aaa authentication auth-mac default group {<group-name>|radius}
no aaa authentication auth-mac default
```

Parameter	Description
<group-name>	Server group name.
radius	Use all RADIUS servers.

Default MAC-based Port Authentication is disabled by default.

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command

All configured RADIUS Servers are automatically members of the server group **radius**. If a server is added to a named group **<*group-name*>**, it also remains a member of the group **radius**.

Examples To enable MAC-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group
radius
```

To disable MAC-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac default
```

Related Commands
aaa accounting auth-mac default
auth-mac enable

aaa authentication auth-web

This command enables Web-based Port Authentication globally and allows you to enable an authentication method list (in this case, a list of RADIUS Servers). It is automatically applied to every interface running Web-based Port Authentication.

Use the **no** variant of this command to globally disable Web-based Port Authentication.

Syntax

```
aaa authentication auth-web default group {<group-name>|radius}
no aaa authentication auth-web default
```

Parameter	Description
<group-name>	Server group name.
radius	Use all RADIUS servers.

Default Web-based Port Authentication is disabled by default.

Mode Global Configuration

Usage There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group <*group-name*>** : use the specified RADIUS server group configured with the **aaa group server** command

Note that you need to configure an IPv4 address for the VLAN interface on which We Authentication is running.

Examples To enable Web-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group
radius
```

To disable Web-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

Related Commands **aaa accounting auth-web default**
auth-mac enable

aaa authentication dot1x

This command enables 802.1X-based Port Authentication globally and allows you to enable an authentication method list. It is automatically applied to every interface running 802.1X-based Port Authentication.

Use the **no** variant of this command to globally disable 802.1X-based Port Authentication.

Syntax

```
aaa authentication dot1x default group {<group-name>|radius}
no aaa authentication dot1x default
```

Parameter	Description
`radius`	Use all RADIUS servers.
<group-name>	Server group name.

Default 802.1X-based Port Authentication is disabled by default.

Mode Global Configuration

Usage Use this command to specify the default method list to use for authentication on all switch ports with 802.1X enabled. Use the **no** variant of this command to reset the authentication method list for 802.1X to its default (i.e. to use the group **radius**, containing all RADIUS servers configured by the **radius-server host** command).

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by **radius-server host** command
- **group *<group-name>*** : use the specified RADIUS server group configured with the **aaa group server** command

Examples To enable 802.1X-based Port Authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x default group radius
```

To disable 802.1X-based Port Authentication, use the command:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default
```

Related Commands

aaa accounting dot1x
aaa group server
dot1x port-control
radius-server host

aaa authentication enable default group tacacs+

This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated against the TACACS+ server.

Use the **no** variant of this command to disable privilege level authentication.

Syntax

```
aaa authentication enable default group tacacs+ [local] [none]
no aaa authentication enable default
```

Parameter	Description
`local`	Use the locally configured enable password (**enable password** command) for authentication.
`none`	No authentication.

Default Local privilege level authentication is enabled by default (**aaa authentication enable default local** command).

Mode Global Configuration

Usage A user is configured on a TACACS+ server with a maximum privilege level. When they enter the **enable (Privileged Exec mode)** command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

Note If both **local** and **none** are specified, you must always specify **local** first.

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**
  then the user is never granted access to Privileged Exec mode.
- **aaa authentication enable default group tacacs+ local**
  then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command), then the enable authentication will fail until the TACACS+ server becomes available again.
- **aaa authentication enable default group tacacs+ none**
  then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.
- **aaa authentication enable default group tacacs+ local none**
  then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

Examples

To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related Commands

aaa authentication login
aaa authentication enable default local
enable (Privileged Exec mode)
enable password
enable secret
tacacs-server host

aaa authentication enable default local

This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated locally.

Syntax `aaa authentication enable default local`

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

Usage The privilege level configured for a particular user in the local user database is the privilege threshold above which the user is prompted for an **enable (Privileged Exec mode)** command.

Examples To enable local privilege level authentication command, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related Commands
aaa authentication enable default group tacacs+
aaa authentication login
enable (Privileged Exec mode)
enable password
enable secret
tacacs-server host

aaa authentication login

Use this command to create an ordered list of methods to use to authenticate user login, or to replace an existing method list with the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the **login authentication** command. To apply a non-default method list, you must also use the **login authentication** command.

Use the **no** variant of this command to remove an authentication method list for user login. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

Syntax

```
aaa authentication login {default|<list-name>}
   {[local] [group {radius|tacacs+|<group-name>}]}

no aaa authentication login {default|<list-name>}
```

Parameter	Description
`default`	Set the default authentication server for user login.
<list-name>	Name of authentication server.
`local`	Use the local username database.
`group`	Use server group.
`radius`	Use all RADIUS servers configured by the **radius-server host** command on page 49.6.
`tacacs+`	Use all TACACS+ servers configured by the **tacacs-server host** command.
<group-name>	Use the specified RADIUS server group, as configured by the **aaa group server** command.

Default If the default server is not configured using this command, user login authentication uses the local user database only.

If the **default** method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the **login authentication** command.

local is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. Reset to the default method list using the **no aaa authentication login default** command.

Mode Global Configuration

Usage When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies group tacacs+ local, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers not the local user database; the user login fails.

Examples To configure the default authentication method list for user login to use first all available RADIUS servers for user login authentication 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 method list called `USERS` to use first the RADIUS server group `RAD_GROUP1` for user login authentication and then the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group
RAD_GROUP1 local
```

To configure a user login authentication method list called `USERS` to use first the TACACS+ servers for user login authentication and then the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login default
```

To delete an existing authentication method list `USERS` created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related Commands

aaa accounting commands
aaa authentication enable default group tacacs+
login authentication

aaa group server

This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in **aaa** commands. The group name **radius** is predefined, which includes all RADIUS servers configured by the **radius-server host** command.

RADIUS servers are added to a server group using the **server** command. Each RADIUS server should be configured using the **radius-server host** command.

Use the **no** variant of this command to remove an existing RADIUS server group.

Syntax

```
aaa group server radius <group-name>
no aaa group server radius <group-name>
```

Parameter	Description
<group-name>	Server group name.

Mode Global Configuration

Usage Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the **radius-server host** command. To add RADIUS servers to a server group, use the **server** command.

Examples To create a RADIUS server group named `GROUP1` with hosts `192.168.1.1`, `192.168.2.1` and `192.168.3.1`, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named `GROUP1` from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

Related Commands

aaa accounting auth-mac default
aaa accounting auth-web default
aaa accounting dot1x
aaa accounting login
aaa authentication auth-mac
aaa authentication auth-web
aaa authentication dot1x
aaa authentication login
radius-server host
server (Server Group)

aaa local authentication attempts lockout-time

This command configures the duration of the user lockout period.

Use the **no** variant of this command to restore the duration of the user lockout period to its default of 300 seconds (5 minutes).

Syntax

```
aaa local authentication attempts lockout-time <lockout-tiime>
no aaa local authentication attempts lockout-time
```

Parameter	Description
<lockout-time>	<0-10000>. Time in seconds to lockout the user.

Mode Global Configuration

Default The default for the lockout-time is 300 seconds (5 minutes).

Usage While locked out all attempts to login with the locked account will fail. The lockout can be manually cleared by another privileged account using the **clear aaa local user lockout** command.

Examples To configure the lockout period to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts lockout-time
600
```

To restore the default lockout period of 5 minutes (300 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts
lockout-time
```

Related Commands **aaa local authentication attempts max-fail**

aaa local authentication attempts max-fail

This command configures the maximum number of failed login attempts before a user account is locked out. Every time a login attempt fails the failed login counter is incremented.

Use the **no** variant of this command to restore the maximum number of failed login attempts to the default setting (five failed login attempts).

Syntax

```
aaa local authentication attempts max-fail <failed-logins>
no aaa local authentication attempts max-fail
```

Parameter	Description
<failed-logins>	<1-32>. Number of login failures allowed before locking out a user.

Mode Global Configuration

Default The default for the maximum number of failed login attempts is five failed login attempts.

Usage When the failed login counter reaches the limit configured by this command that user account is locked out for a specified duration configured by the **aaa local authentication attempts lockout-time** command.

When a successful login occurs the failed login counter is reset to 0. When a user account is locked out all attempts to login using that user account will fail.

Examples To configure the number of login failures that will lock out a user account to two login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail 2
```

To restore the number of login failures that will lock out a user account to the default number of login attempts (five login attempts), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
```

Related Commands

aaa local authentication attempts lockout-time
clear aaa local user lockout

accounting login

This command applies a login accounting method list to console or vty lines for user login. When login accounting is enabled using this command, logging events generate an accounting record to the accounting server.

The accounting method list must be configured first using this command. If an accounting method list is specified that has not been created by this command then accounting will be disabled on the specified lines.

The **no** variant of this command resets AAA (Authentication, Authorization, Accounting) Accounting applied to console or vty lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

Syntax

```
accounting login {default|<list-name>}
no accounting login
```

Parameter	Description
`default`	Default accounting method list.
`<list-name>`	Named accounting method list.

Default By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using this command beforehand.

Mode Line Configuration

Examples To apply the accounting server `USERS` to all vty lines use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# accounting login USERS
```

Related Commands
aaa accounting commands
aaa accounting login

clear aaa local user lockout

Use this command to clear the lockout on a specific user account or all user accounts.

Syntax `clear aaa local user lockout {username <username>|all}`

Parameter	Description
`username`	Clear lockout for the specified user.
`<username>`	Specifies the user account.
`all`	Clear lockout for all user accounts.

Mode Privileged Exec

Examples To unlock the user account '`bob`' use the following command:

```
awplus# clear aaa local user lockout username bob
```

To unlock all user accounts use the following command:

```
awplus# clear aaa local user lockout all
```

Related Commands **aaa local authentication attempts lockout-time**

debug aaa

This command enables AAA debugging.

Use the **no** variant of this command to disable AAA debugging.

Syntax

```
debug aaa [accounting|all|authentication|authorization]
no debug aaa [accounting|all|authentication|authorization]
```

Parameter	Description
`accounting`	Accounting debugging.
`all`	All debugging options are enabled.
`authentication`	Authentication debugging.
`authorization`	Authorization debugging.

Default AAA debugging is disabled by default.

Mode Privileged Exec

Examples To enable authentication debugging for AAA, use the command:

```
awplus# debug aaa authentication
```

To disable authentication debugging for AAA, use the command:

```
awplus# no debug aaa authentication
```

Related Commands **show debugging aaa**
undebug aaa

login authentication

Use this command to apply an AAA server for authenticating user login attempts from a console or remote logins on these console or VTY lines. The authentication method list must be specified by the **aaa authentication login** command. If the method list has not been configured by the **aaa authentication login** command, login authentication will fail on these lines.

Use the **no** variant of this command to reset AAA Authentication configuration to use the default method list for login authentication on these console or VTY lines.

Command Syntax

```
login authentication {default|<list-name>}
no login authentication
```

Parameter	Description
`default`	The default authentication method list. If the default method list has not been configured by the **aaa authentication login** command, the local user database is used for user login authentication.
<list-name>	Named authentication server.

Default The default login authentication method list, as specified by the **aaa authentication login** command, is used to authenticate user login. If this has not been specified, the default is to use the local user database.

Mode Line Configuration

Examples To reset user authentication configuration on all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# no login authentication
```

Related Commands
aaa authentication login
line

show aaa local user locked

This command displays the current number of failed attempts, last failure time and location against each user account attempting to log into the device.

Note that once the lockout count has been manually cleared by another privileged account using the **clear aaa local user lockout** command on page 45.28 or a locked account successfully logs into the system after waiting for the lockout time, this command will display nothing for that particular account.

Syntax `show aaa local user locked`

Mode User Exec and Privileged Exec

Example To display the current failed attempts for local users, use the command:

```
awplus# show aaa local user locked
```

Output **Figure 45-1: Example output from the show aaa local user locked command**

```
awplus# show aaa local user locked
Login           Failures Latest failure     From
bob                  3    05/23/14 16:21:37  ttyS0
manager              5    05/23/14 16:31:44  192.168.1.200
```

Related Commands
aaa local authentication attempts lockout-time
aaa local authentication attempts max-fail
clear aaa local user lockout

show debugging aaa

This command displays the current debugging status for AAA (Authentication, Authorization, Accounting).

Syntax `show debugging aaa`

Mode User Exec and Privileged Exec

Example To display the current debugging status of AAA, use the command:

```
awplus# show debug aaa
```

Output **Figure 45-2: Example output from the show debug aaa command**

```
AAA debugging status:
    Authentication debugging is on
    Accounting debugging is off
```

undebug aaa

This command applies the functionality of the **no debug aaa** command on page 45.29.

Chapter 46: 802.1X Introduction and Configuration

Introduction 46.2
802.1X System Components 46.2
The 802.1X Implementation 46.5
Configuring 802.1X 46.6

Introduction

802.1X is an IEEE standard providing a mechanism for authenticating devices attached to a LAN port or wireless device. Devices wishing to access services behind a port must authenticate themselves before any Ethernet packets are allowed to pass through. The protocol is referred to as 802.1X because it was initially defined in the IEEE standard 802.1X, published in 2001 and revised in 2004 and again as the current 802.1X 2010 standard.

Networks have two important requirements:

- Security: Authentication and Authorization
- Flexibility: The ability for users to roam

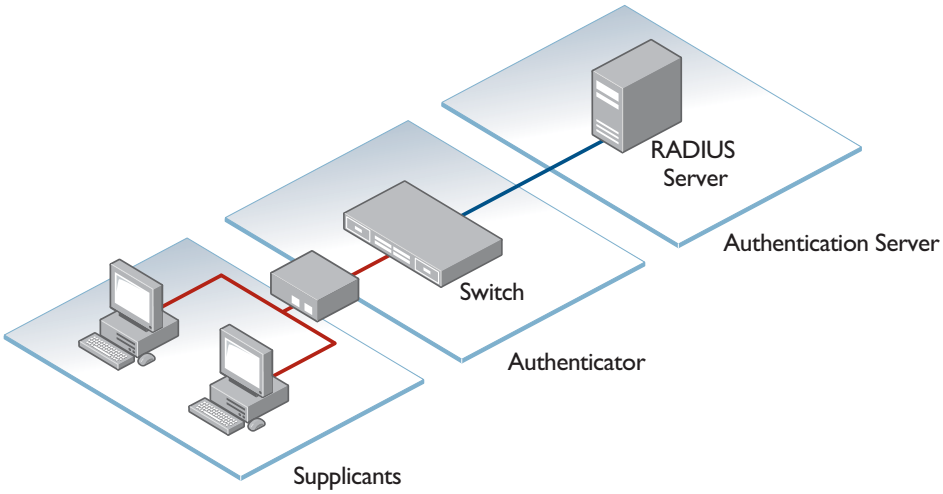
Networks need a device authentication method that is highly secure, but not tied to a port's physical location. Network resources presented to a given user need to be determined from their authentication credentials.

802.1X user authentication satisfies these requirements. It is relatively uncomplicated and has little impact on network performance. It is a protocol that is medium-independent — being equally as effective on wireless connections (802.11i) and wired connections. 802.1X user authentication is rapidly becoming an expected component on networks.

802.1X System Components

There are three main components to a system using 802.1X port authentication control:

- Authenticator: The device that wishes to enforce authentication before allowing access to services that are accessible behind it. An example of this is a switch that has 802.1X port authentication control enabled.
- Supplicant: The client that wishes to access services offered by the authenticator's system. An example of this is a Windows XP Professional PC with an 802.1X client.
- Authentication server: The device that uses the authentication credentials supplied by the supplicant, to determine if the authenticator should grant access to its services. The AlliedWare Plus implementation of 802.1X supports the use of a RADIUS. authentication server using Extensible Authentication Protocol (EAP) in conjunction with RADIUS.

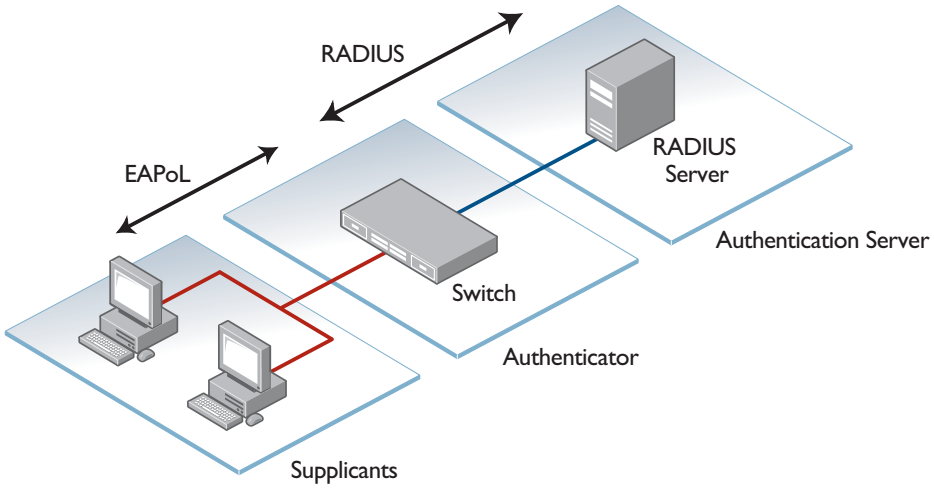


802.1X component protocols

There are two protocols involved in the authentication conversation:

- EAPoL exchanged between the supplicant and authenticator.
  - « EAPoL—Extensible Authentication Protocol over LAN— is the protocol defined in IEEE802.1X.
- RADIUS exchanged between the authenticator and authentication server.
  - « RADIUS has received specific extensions to interoperate with EAPoL.

The diagram below illustrates where EAPoL and RADIUS protocols are used in the authentication conversation:

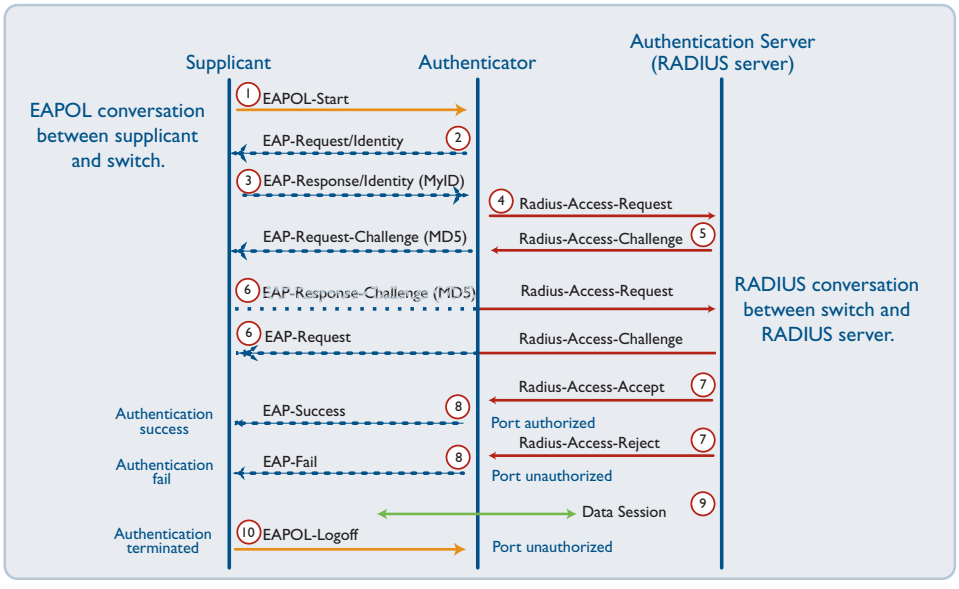


Basic steps in an 802.1X conversation

Step	Action
1	The supplicant informs the authenticator that it wants to initiate the conversation.
2	The authenticator requests the supplicant's credentials.
3	The supplicant sends username/password or X.509 certificate.
4	The authenticator wraps the supplicant's reply into a RADIUS packet and sends it to the RADIUS server.
5	The RADIUS server chooses an authentication method, and sends an appropriate request to the supplicant as a 'challenge'.
6	The RADIUS server and supplicant exchange some messages, ferried by the authenticator.
7	The RADIUS server eventually decides if the supplicant is allowed access and the RADIUS server sends an Access-Accept or Access-Reject message to the Authenticator.
8	The authenticator sends an EAPoL-Success or EAPoL-Fail to the supplicant.
9	The supplicant has a session using the network (if accepted).
10	When the session is over, the supplicant sends a log-off message.

Example message sequence

The diagram below illustrates an exchange using the EAP-MD5 authentication method, which is the simplest authentication method supported by 802.1X. The EAPoL log-off message, of course, is not sent immediately after the other messages in the diagram, but is sent later on, at the end of the supplicant's data session, when it wishes to disconnect from the network.The EAPoL log-off message, of course, is not sent immediately after the other messages in the diagram, but is sent later on, at the end of the supplicant's data session, when it wishes to disconnect from the network.



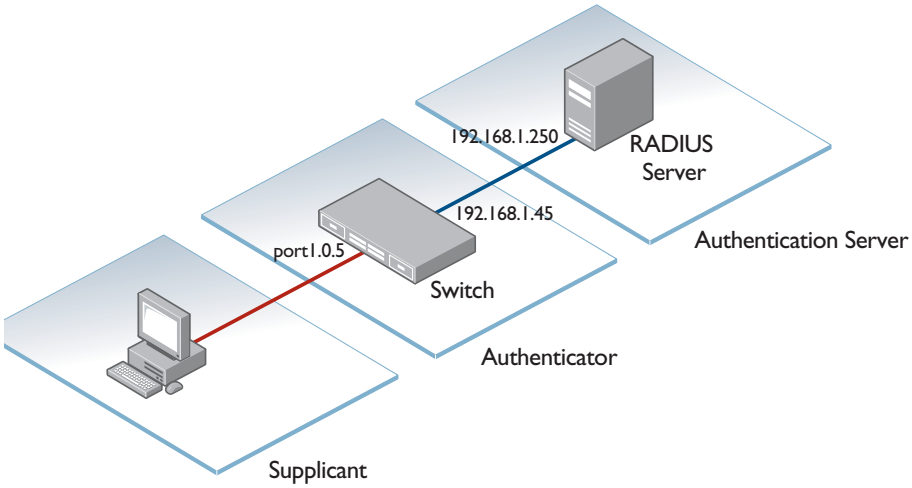
The 802.1X Implementation

802.1X port access control is achieved by making devices attached to a controlled port authenticate themselves via communication with an authentication server before these devices are allowed to access the network behind the controlled port.

Authentication is required on a per-port basis. The main components of an 802.1X implementation are:

- the authenticator - the port on this device that wishes to enforce authentication before allowing access to services that are accessible behind it.
- the supplicant - the port that wishes to access services offered by the authenticator's system. The supplicant may be a port on a PC or other device connected to this device.
- the authentication server - a device that uses the authentication credentials supplied by the supplicant, via the authenticator, to determine if the authenticator should grant access to its services.

To configure the switch operating as authenticator, follow the instructions below:



1. Configure a RADIUS server for the switch to send requests to

```
awplus(config)# radius-server host 192.168.1.250 key
                <secret-key>
```

2. Instruct 802.1X to use the configured RADIUS server

```
awplus(config)# aaa authentication dot1x default group radius
```

3. Configure port1.0.5 for 802.1X authentication

```
   awplus(config)# interface port1.0.5
awplus(config-if)# dot1x port-control auto
awplus(config-if)# spanning-tree portfast
```

Configuring 802.1X

The following example explains how to configure 802.1X. In this example, the RADIUS Server keeps the Client information, validating the identity of the Client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client.

To configure 802.1X authentication, first enable authentication on `port1.0.1` and `port1.0.2` and then specify the RADIUS Server IP address and port.

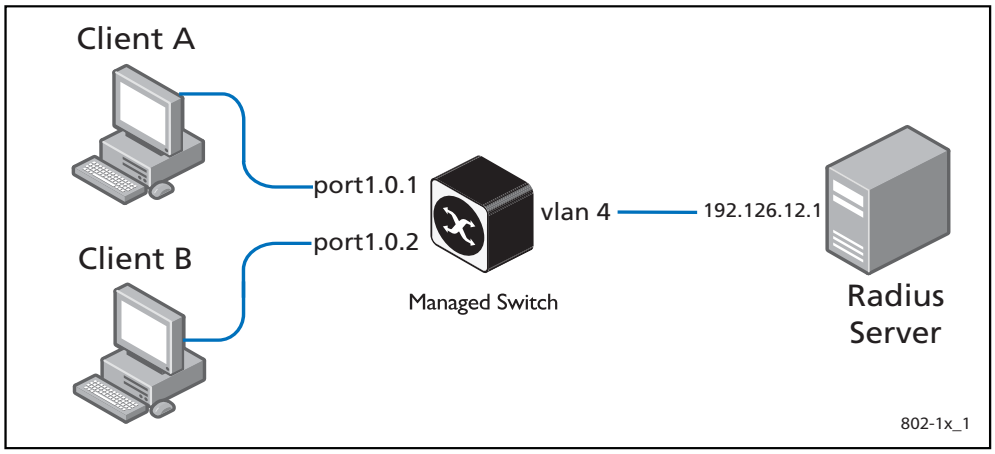


Table 46-1: 802.1X configuration on the switch

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `aaa authentication dot1x default group radius`	Enable authentication globally.
`awplus(config)#` `interface port1.0.1`	Specify the interface (`port1.0.1`) to be configured and enter the Interface mode.
`awplus(config-if)#` `dot1x port-control auto`	Enable authentication (via RADIUS) on `port1.0.1`.
`awplus(config-if)#` `dot1x control-direction both`	Block traffic in both directions, other than authentication packets, until authentication is complete.
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.
`awplus(config)#` `interface port1.0.2`	Specify the interface (`port1.0.2`) you are configuring and enter the Interface mode.
`awplus(config-if)#` `dot1x port-control auto`	Enable authentication (via RADIUS) on `port1.0.2`.

Table 46-1: 802.1X configuration on the switch (cont.)

`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.
`awplus(config)#`	
`radius-server host 192.126.12.1 auth-port 1812`	Specify the RADIUS Server address (`192.126.12.1`) and authentication port.
`awplus(config)#`	
`radius-server key secret`	Specify the shared key `secret` between the RADIUS server and the client.
`awplus(config)#`	
`interface vlan4`	Specify the vlan (`vlan4`) to be configured and enter the Interface mode.
`awplus(config-if)#`	
`ip address 192.126.12.2/24`	Set the IP address on `vlan4`.

Names of commands used
dot1x port-control
radius-server host
radius-server key

Validation Commands
show dot1x
show dot1x interface

Chapter 47: 802.1X Commands

Command List 47.2
debug dot1x 47.2
dot1x control-direction 47.3
dot1x eap 47.4
dot1x eapol-version 47.5
dot1x initialize interface 47.6
dot1x initialize supplicant 47.7
dot1x keytransmit 47.8
dot1x max-auth-fail 47.9
dot1x max-reauth-req 47.11
dot1x port-control 47.12
dot1x timeout tx-period 47.14
show debugging dot1x 47.15
show dot1x 47.16
show dot1x diagnostics 47.18
show dot1x interface 47.19
show dot1x sessionstatistics 47.24
show dot1x statistics interface 47.25
show dot1x supplicant 47.26
show dot1x supplicant interface 47.28
undebug dot1x 47.31

Command List

This chapter provides an alphabetical reference of commands used to configure 802.1X port access control.

debug dot1x

Use this command to enable 802.1X IEEE Port-Based Network Access Control troubleshooting functions.

Use the **no** variant of this command to disable this function.

Syntax

```
debug dot1x [all|auth-web|event|nsm|packet|timer]
no debug all dot1x
no debug dot1x [all|auth-web|event|nsm|packet|timer]
```

Parameter	Description
`all`	Used with the **no** variant of this command exclusively; turns off all debugging for 802.1X.
`auth-web`	Specifies debugging for 802.1X auth-web information.
`events`	Specifies debugging for 802.1X events.
`nsm`	Specifies debugging for NSM messages.
`packet`	Specifies debugging for 802.1X packets.
`timer`	Specifies debugging for 802.1X timers.

Mode Privileged Exec and Global Configuration

Usage 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**
undebug dot1x

dot1x control-direction

This command sets the direction of the filter for the unauthorized interface.

If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the ingress packets received from the supplicant.

If the optional **both** parameter is specified with this command then packets entering (ingress) and leaving (egress) the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.

The **no** variant of this command sets the direction of the filter to **both**. The port will then discard both ingress and egress traffic.

Syntax

```
dot1x control-direction {in|both}
no dot1x control-direction
```

Parameter	Description
`in`	Discard received packets from the supplicant (ingress packets).
`both`	Discard received packets from the supplicant (ingress packets) and transmitted packets to the supplicant (egress packets).

Default The authentication port direction is set to **both** by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Example s To set the port direction to the default (**both**) for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x control-direction
```

To set the port direction to **in** for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x control-direction in
```

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
`discard`	Discard.
`forward`	Forward to all ports on the switch.
`forward-untagged-vlan`	Forward to ports with the same untagged VLAN.
`forward-vlan`	Forward to ports with the same VLAN.

Default The transmit mode is set to `discard` EAP packets by default.

Mode Global Configuration

Examples To set the transmit mode of EAP packet to `forward` to forward EAP packets to all ports on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward
```

To set the transmit mode of EAP packet to `discard` to discard EAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap discard
```

To set the transmit mode of EAP packet to `forward-untagged-vlan` to forward EAP packets to ports with the same untagged vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to `forward-vlan` to forward EAP packets to ports with the same vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-vlan
```

dot1x eapol-version

This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the **no** variant of this command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

Syntax

```
dot1x eapol-version {1|2}
no dot1x eapol-version
```

Parameter	Description
1	EAPOL version.
2	EAPOL version.

Default The EAP version for 802.1X authentication is set to 1 by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples To set the EAPOL protocol version to `2` for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x eapol-version
```

Validation Commands **show dot1x**
show dot1x interface

dot1x initialize interface

This command removes authorization for a connected **interface** with the specified *<interface-list>*. The connection will attempt to re-authorize when the specified **port** attempts to make use of the network connection.

Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the interface trying to access the network resources.

Syntax `dot1x initialize interface <interface-list>`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.2-1.0.4`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Examples To initialize 802.1X port authentication on the interface `port1.0.2`, use the command:

```
awplus# dot1x initialize interface port1.0.2
```

To unauthorize switch `port1.0.1` and attempt reauthentication on switch `port1.0.1`, use the command:

```
awplus# dot1x initialize interface port1.0.1
```

To unauthorize all switch ports for a 24-port device and attempt reauthentication, use the command:

```
awplus# dot1x initialize interface port1.0.1-port1.0.24
```

Validation Commands **show dot1x**
show dot1x interface

Related Commands **dot1x initialize supplicant**

dot1x initialize supplicant

This command removes authorization for a connected *supplicant* with the specified **MAC address** or **username**. The connection will attempt to re-authorize when the specified supplicant attempts to make use of the network connection.

Note Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the supplicant trying to access the network resources.

Syntax `dot1x initialize supplicant {<macadd>|username}`

Parameter	Description
`dot1x`	IEEE 802.1X Port-Based Access Control.
`initialize`	Initialize the port to attempt reauthentication.
`supplicant`	Specify the supplicant to initialize.
<macadd>	MAC (hardware address of the supplicant.
`username`	The name of the supplicant entry.

Mode Privileged Exec

Example To initialize the supplicant authentication, use the commands

```
awplus# configure terminal
awplus(config)# dot1x initialize supplicant
0090.99ab.a020
awplus(config)# dot1x initialize supplicant guest
```

Validation Commands **show dot1x**
show dot1x supplicant

Related Commands **dot1x initialize interface**

dot1x keytransmit

This command enables key transmission on the interface specified previously in Interface mode.

The **no** variant of this command disables key transmission on the interface specified.

Syntax

```
dot1x keytransmit
no dot1x keytransmit
```

Default Key transmission for port authentication is enabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use this command to enable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant. Use the **no** variant of this command to disable key transmission.

Examples To enable the key transmit feature on interface `port1.0.2`, after it has been disabled by negation, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x keytransmit
```

To disable the key transmit feature from the default startup configuration on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x keytransmit
```

Validation Commands **show dot1x**
show dot1x interface

dot1x max-auth-fail

Use this command to configure the maximum number of login attempts for a supplicant (client device) using the **auth-fail vlan** feature, when using 802.1X port authentication on an interface.

The **no** variant of this command resets the maximum login attempts for a supplicant (client device) using the auth-fail vlan feature, to the default configuration of 3 login attempts.

Syntax

```
dot1x max-auth-fail <0-10>
no dot1x max-auth-fail
```

Parameter	Description
<0-10>	Specify the maximum number of login attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum number of login attempts for a supplicant on an interface using 802.1X port authentication is three (3) login attempts.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage This command sets the maximum number of login attempts for supplicants on an interface. The supplicant is moved to the auth-fail VLAN from the Guest VLAN after the number of failed login attempts using 802.1X authentication is equal to the number set with this command.

See the related **auth auth-fail vlan** command on page 43.3. See also the section **"Failed Authentication VLAN" on page 42.35** for information about the auth-fail VLAN feature.

See the section **"Limitations on Allowed Feature Combinations" on page 42.35** for information about restrictions regarding combinations of authentication enhancements working together.

Examples To configure the maximum number of login attempts for a supplicant on interface `port1.0.2` to a single (`1`) login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on interface `port1.0.2` to the default number of three (`3`) login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-auth-fail
```

Validation Commands **show running-config**

Related Commands

auth auth-fail vlan
dot1x max-reauth-req
show dot1x interface

dot1x max-reauth-req

This command sets the number of reauthentication attempts before an interface is unauthorized.

The **no** variant of this command resets the reauthentication delay to the default.

Syntax

```
dot1x max-reauth-req <1-10>
no dot1x max-reauth-req
```

Parameter	Description
<1-10>	Specify the maximum number of reauthentication attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum reauthentication attempts for interfaces using 802.1X port authentication is two (2) reauthentication attempts, before an interface is unauthorized.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use this command to set the maximum reauthentication attempts after failure.

Examples To configure the maximum number of reauthentication attempts for interface `port1.0.2` to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for interface `port1.0.2` to the default maximum number of two (2) reauthentication attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-reauth-req
```

Validation Commands **show running-config**

Related Commands **dot1x max-auth-fail**
show dot1x interface

dot1x port-control

This command enables 802.1X port authentication on the interface specified, and sets the control of the authentication port. When **port-control** is set to **auto**, the 802.1X authentication feature is executed on the interface, but only if the **aaa authentication dot1x** command has been issued.

The **no** variant of this command disables the port authentication on the interface specified.

Syntax

```
dot1x port-control {force-unauthorized|force-authorized|auto}
no dot1x port-control
```

Parameter	Description
`force-unauthorized`	Force port state to unauthorized. Specify to force a port to always be in an unauthorized state.
`force-authorized`	Force port state to authorized. Specify to force a port to always be in an authorized state.
`auto`	Allow port client to negotiate authentication. Specify to enable authentication on port.

Default 802.1X port control is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use this command to force a port state. Note that all **dot1x** commands can only be applied to switch ports. They cannot be applied to dynamic (LACP) or static channel groups.

Examples To enable port authentication on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
```

To enable port authentication force authorized on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control force-authorized
```

To disable port authentication on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x port-control
```

Validation Commands **show dot1x interface**

Related Commands **aaa authentication dot1x**

dot1x timeout tx-period

This command sets the transmit timeout for the authentication request on the specified interface.

The **no** variant of this command resets the transmit timeout period to the default (30 seconds).

Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter	Description
<1-65535>	Seconds.

Default The default transmit period for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use this command to set the interval between successive attempts to request an ID.

Examples To set the transmit timeout period to 5 seconds on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x timeout tx-period
```

Validation Commands **show dot1x**
show dot1x interface

show debugging dot1x

Use this command to display the 802.1X debugging option set.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show debugging dot1x`

Mode User Exec and Privileged Exec

Usage This is a sample output from the `show debugging dot1x` command.

```
awplus# debug dot1x

awplus# show debugging dot1x

802.1X debugging status:
  802.1X events debugging is on
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

Example

```
awplus# show debugging dot1x
```

Related Commands **debug dot1x**

show dot1x

This command shows authentication information for dot1x (802.1X) port authentication.

If you specify the optional **all** parameter then this command also displays all authentication information for each port available on the switch.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x [all]`

Parameter	Description
`all`	Displays all authentication information for each port available on the switch.

Mode Privileged Exec

Example

```
awplus# show dot1x all
```

Figure 47-1: Example output from the show dot1x command

```
awplus# show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 150.87.18.89:1812
Next radius message id: 5
RADIUS client address: not configured
Authentication info for interface port1.0.6
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
PAE: connectTimeout: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
dynamicVlanCreation: single-dynamic-vlan
assignFailActionRule: deny
hostMode: multi-supplicant
maxSupplicant: 1024
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
twoStepAuthentication:
    configured: enabled
    actual: enabled
SupplicantMac: none
```

Figure 47-1: Example output from the show dot1x command (cont.)

```
supplicantMac: none
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
    authenticationMethod: 802.1X Authentication
    portStatus: Authorized - currentId: 1
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
    BE: state: Idle - reqCount: 0 - idFromServer: 0
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    criticalState: off
    dynamicVlanId: 2
802.1X statistics for interface port1.0.6
    EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
    EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
    EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
    EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
    Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
    EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src:  00d0.59ab.7037
Authentication session statistics for interface port1.0.6
    session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminate cause: Not terminated yet
Authentication Diagnostics for interface port1.0.6
    Supplicant address: 00d0.59ab.7037
    authEnterConnecting: 2
    authEaplogoffWhileConnecting: 1
    authEnterAuthenticating: 2
    authSuccessWhileAuthenticating: 1
    authTimeoutWhileAuthenticating: 1
    authFailWhileAuthenticating: 0
    authEapstartWhileAuthenticating: 0
    authEaplogoggWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
    BackendAuthFails: 0
```

show dot1x diagnostics

This command shows 802.1X authentication diagnostics for the specified interface (optional), which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x diagnostics [interface <interface-list>]`

Parameter	Description
`interface`	Specify a port to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.2-1.0.4`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See the sample output below showing 802.1X authentication diagnostics for `port1.0.5`:

```
awplus# show dot1x diagnostics interface port1.0.5
```

Output **Figure 47-2: Example output from the show dot1x diagnostics command**

```
Authentication Diagnostics for interface port1.0.5
   Supplicant address: 00d0.59ab.7037
     authEnterConnecting: 2
     authEaplogoffWhileConnecting: 1
     authEnterAuthenticating: 2
     authSuccessWhileAuthenticating: 1
     authTimeoutWhileAuthenticating: 1
     authFailWhileAuthenticating: 0
     authEapstartWhileAuthenticating: 0
     authEaplogoggWhileAuthenticating: 0
     authReauthsWhileAuthenticated: 0
     authEapstartWhileAuthenticated: 0
     authEaplogoffWhileAuthenticated: 0
     BackendResponses: 2
     BackendAccessChallenges: 1
     BackendOtherrequestToSupplicant: 3
     BackendAuthSuccess: 1
```

show dot1x interface

This command shows the status of 802.1X port-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interfaces. Use the optional **statistics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **supplicant** parameter to show the supplicant state for the specified interfaces.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax

```
show dot1x interface <interface-list> [diagnostics|sessionstatistics|
    statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.3-1.0.5`. Do not mix interface types in a list The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session Statistics.
`statistics`	Statistics.
`supplicant`	Supplicant.
`brief`	Brief summary of supplicant state.

Mode Privileged Exec

Examples See the sample output below showing 802.1X authentication status for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6
```

Figure 47-3: Example output from the show dot1x interface command for a port

```
awplus#show dot1x interface port1.0.6
Authentication info for interface port1.0.6
    portEnabled: true - portControl: Auto
    portStatus: Authorized
    reAuthenticate: disabled
    reAuthPeriod: 3600
    PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
    PAE: connectTimeout: 30
    BE: suppTimeout: 30 - serverTimeout: 30
    CD: adminControlledDirections: in
    KT: keyTxEnabled: false
    critical: disabled
    guestVlan: disabled
    dynamicVlanCreation: single-dynamic-vlan
        assignFailActionRule: deny
    hostMode: multi-supplicant
        maxSupplicant: 1024
    dot1x: enabled
        protocolVersion: 1
    authMac: enabled
        method: PAP
        reauthRelearning: disabled
    authWeb: enabled
        method: PAP
        lockCount: 3
        packetForwarding: disabled
     twoStepAuthentication:
        configured: enabled
        actual: enabled
supplicantMac: none
```

See the sample output below showing 802.1X authentication `sessionstatistics` for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 sessionstatistics
```

```
awplus#show dot1x interface port1.0.6 sessionstatistics
Authentication session statistics for interface port1.0.6
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

See sample output below showing 802.1X authentication `diagnostics` for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 diagnostics
```

```
awplus#show dot1x interface port1.0.6 diagnostics
Authentication Diagnostics for interface port1.0.6
    Supplicant address: 00d0.59ab.7037
        authEnterConnecting: 2
        authEaplogoffWhileConnecting: 1
        authEnterAuthenticating: 2
        authSuccessWhileAuthenticating: 1
        authTimeoutWhileAuthenticating: 1
        authFailWhileAuthenticating: 0
        authEapstartWhileAuthenticating: 0
        authEaplogoggWhileAuthenticating: 0
        authReauthsWhileAuthenticated: 0
        authEapstartWhileAuthenticated: 0
        authEaplogoffWhileAuthenticated: 0
        BackendResponses: 2
        BackendAccessChallenges: 1
        BackendOtherrequestToSupplicant: 3
        BackendAuthSuccess: 1
```

See sample output below showing the `supplicant` on the interface `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 supplicant
```

```
awplus#show dot1x interface port1.0.6 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 802.1X (`dot1x`) authentication statistics for `port1.0.6`:

```
awplus# show dot1x statistics interface port1.0.6
```

```
awplus#show dot1x statistics interface port1.0.6
802.1X statistics for interface port1.0.6
    EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
    EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
    EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
    EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
    Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
    EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

Table 47-1: Parameters in the output of the show dot1x interface command

Parameter	Description
`portEnabled`	Interface operational status (Up-true/down-false).
`portControl`	Current control status of the port for 802.1X control.
`portStatus`	802.1X status of the port (authorized/unauthorized).
`reAuthenticate`	Reauthentication enabled/disabled status on port.
`reAuthPeriod`	Value holds meaning only if reauthentication is enabled.
`abort`	Indicates that authentication should be aborted when set to true.
`fail`	Indicates failed authentication attempt when set to false.
`start`	Indicates authentication should be started when set to true.
`timeout`	Indicates authentication attempt timed out when set to true.
`success`	Indicates authentication successful when set to true.
`state`	Current 802.1X operational state of interface.
`mode`	Configured 802.1X mode.
`reAuthCount`	Reauthentication count.
`quietperiod`	Time between reauthentication attempts.
`reAuthMax`	Maximum reauthentication attempts.
`BE`	Backend authentication state machine variables and constants.
`state`	State of the state machine.
`reqCount`	Count of requests sent to server.
`suppTimeout`	Supplicant timeout.
`serverTimeout`	Server timeout.
`maxReq`	Maximum requests to be sent.
`CD`	Controlled Directions State machine.
`adminControlledDirections`	Administrative value (Both/In).

Table 47-1: Parameters in the output of the show dot1x interface command (cont.)

Parameter	Description
`operControlledDirections`	Operational Value (Both/In).
`KR`	Key receive state machine.
`rxKey`	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted.
`KT`	Ket Transmit State machine.
`keyAvailable`	False when key has been transmitted by authenticator, true when new key is available for key exchange.
`keyTxEnabled`	Key transmission enabled/disabled status.

Related Commands

show auth-web diagnostics
show dot1x sessionstatistics
show dot1x statistics interface
show dot1x supplicant interface

show dot1x sessionstatistics

This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x sessionstatistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify a port to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See sample output below showing 802.1X (`dot1x`) authentication session statistics for `port1.0.6`:

```
awplus# show dot1x sessionstatistics interface port1.0.6
```

```
Authentication session statistics for interface port1.0.6
    session user name: manager
        session authentication method: Remote server
        session time: 19440 secs
        session terminat cause: Not terminated yet
```

show dot1x statistics interface

This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x statistics interface <interface-list>`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See sample output below showing 802.1X authentication statistics for `port1.0.6`:

```
awplus# show dot1x statistics interface port1.0.6
```

```
802.1X statistics for interface
   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.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x supplicant [<macadd>] [brief]`

Parameter	Description
<macadd>	MAC (hardware) address of the Supplicant.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Example See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus# show dot1x supplicant
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
    authenticationMethod: dot1x
     Two-Step Authentication:
       firstAuthentication: Pass - Method: mac
       secondAuthentication: Pass - Method: dot1x
portStatus: Authorized - currentId: 4
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.6
   authenticationMethod: dot1x
   totalSupplicantNum: 1
   authorizedSupplicantNum: 1
       macBasedAuthenticationSupplicantNum: 0
       dot1xAuthenticationSupplicantNum: 1
       webBasedAuthenticationSupplicantNum: 0
Interface   VID Mode MAC Address     Status        IP Address     Username
=========   === ==== ===========     ======        ==========     ========
port1.0.6   2   D    00d0.59ab.7037  Authenticated 192.168.2.201  manager
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant brief
```

For example, if two-step authentication is configured with 802.1X authentication as the first method and web authentication as the second method then the output is as follows:

```
Interface port1.0.6
  authenticationMethod: dot1x/web
  Two-Step Authentication
    firstMethod: dot1x
    secondMethod: web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== ========
port1.0.6   5    W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

Related Commands **show dot1x supplicant interface**

show dot1x supplicant interface

This command shows the supplicant state of the authentication mode set for the interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

This command shows a summary when the optional **brief** parameter is used.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dot1x supplicant interface <interface-list> [brief]`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: ■ an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) ■ a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` ■ a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Examples See sample output below showing the supplicant on the interface `port1.0.6`:

```
awplus# show dot1x interface port1.0.6
```

```
Interface port1.0.6
 authenticationMethod: dot1x
  totalSupplicantNum: 1
 authorizedSupplicantNum: 1
   macBasedAuthenticationSupplicantNum: 0
   dot1xAuthenticationSupplicantNum: 1
   webBasedAuthenticationSupplicantNum: 0
   otherAuthenticationSupplicantNum: 0

 Supplicant name: VCSPCVLAN10
 Supplicant address: 0000.cd07.7b60
   authenticationMethod: 802.1X
 Two-Step Authentication:
   firstAuthentication: Pass - Method: mac
   secondAuthentication: Pass - Method: dot1x
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections:in -
operControlledDirections:in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant interface brief
```

```
Interface port1.0.6
    authenticationMethod: dot1x
Two-Step Authentication:
   firstMethod: mac
   secondMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address     Status          IP Address      Username
=========   ===  ==== ===========     ======          ==========      ========
port1.0.6   2    D    00d0.59ab.7037  Authenticated   192.168.2.201   manager
```

See the sample output below for static channel group (static aggregator) interface `sa1`:

```
awplus# show dot1x interface sa1 supplicant brief
```

```
awplus#show dot1x interface sa1 supplicant brief
Interface sa1
  authenticationMethod: dot1x
Two-Step Authentication:
   firstMethod: mac
   secondMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
     dot1xAuthenticationSupplicantNum: 1
     webBasedAuthenticationSupplicantNum: 0
     otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========   ==== ==== ============== ================= =============== ========
sa1         1    D    00d0.59ab.7037 Authenticated     --              test1
```

Related Commands **show dot1x supplicant**

undebug dot1x

This command applies the functionality of the **no debug dot1x** command on page 47.2.

Chapter 48: RADIUS Introduction and Configuration

Introduction 48.2
RADIUS Packets 48.3
RADIUS Attributes 48.4
RADIUS Security 48.5
RADIUS Proxy 48.6
RADIUS Accounting 48.7
RADIUS Configuration 48.9
Switch Configuration Tasks 48.9
Switch to RADIUS Server Communication 48.10
AAA Server Groups Configuration 48.12
RADIUS Configuration Examples 48.15
RADIUS Authentication 48.15
Single RADIUS Server Configuration 48.16
Multiple RADIUS Server Configuration 48.17
RADIUS Server Group Configuration 48.17
RADIUS Server Configuration using Server Groups 48.18

Introduction

The main purpose of RADIUS (Remote Authentication Dial In User Service) is to enable the authentication of network users stored in a database on a server known as a RADIUS Server.

When users connect to the network, the switch the users connect to can challenge the users for authentication, and pass on the authentication to the RADIUS server to check. Based on the result of the check against the database, the RADIUS Server informs the switch whether or not to allow the connected user access to the network.

A RADIUS Server can do more than allow or deny access to the network. A RADIUS Server can send back parameters to the connected users, such as an IP address for the user, or a VLAN for the user, or a privilege level for a session. RADIUS also provides an accounting service. Switches can inform the RADIUS Server how long a user has been connected to the network, and how much traffic the user has sent and received while connected to the network.

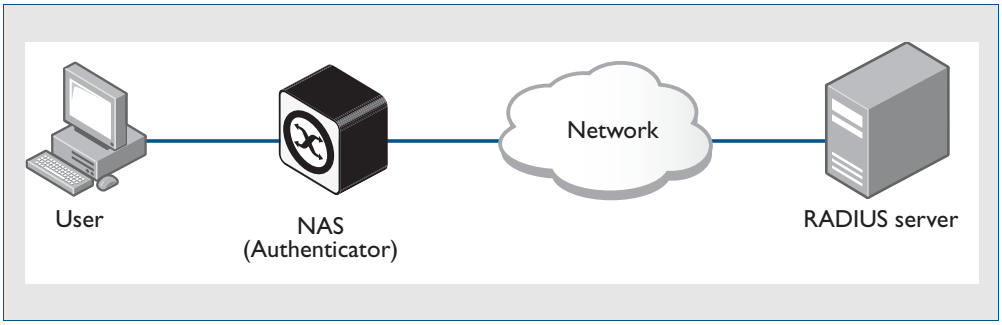
The original use for RADIUS was for the authentication of users dialing into an ISP (Internet Service Provider). A PPP (Point-to-Point Protocol) connection would be established between the remote client and the ISP's access switch. The ISP's access switch would receive the client's username and password using PAP (Password Authentication Protocol) or using CHAP (Challenge Handshake Authentication Protocol) and pass on the client's username and password to the RADIUS server to authenticate the client. The RADIUS Server's response to the authentication request would be sent back to the client as a PAP or CHAP allow or deny.

RADIUS has been adapted to network access authentication applications. Network access authentication using RADIUS follows a similar method to the PPP dial-up application for ISPs. For general network access authentication there is the RADIUS Server where the database of user authentication data is stored and a NAS (Network Access Server), which is the switch that user connects to first. The RADIUS Server and the NAS communicate with each other through exchanging attributes. Usernames and passwords are treated as attributes in RADIUS packets to and from a RADIUS Server and a NAS. The RADIUS Server is configured with a list of valid NASs that are allowed to send authentication requests to the RADIUS Server.

The RADIUS Server will not accept authentication requests from a NAS that is not on the list of valid NASs. Each NAS has a shared secret, which is a shared key with the RADIUS Server that is used to authenticate requests. The RADIUS Server has access to a list of user authentication data, stored within the RADIUS Server or accessed from another server.

Communication between the NAS and RADIUS Server uses the RADIUS protocol. The RADIUS protocol uses UDP packets. There are two UDP ports used as the destination port for RADIUS authentication packets (ports 1645 and 1812). Note that port 1812 is in more common use than port 1645 for authentication packets. UDP ports (ports 1646 and 1813) are used for RADIUS accounting separately from the ports used for RADIUS authentication.

Figure 48-1: Example showing a user to a NAS to a RADIUS server network connection



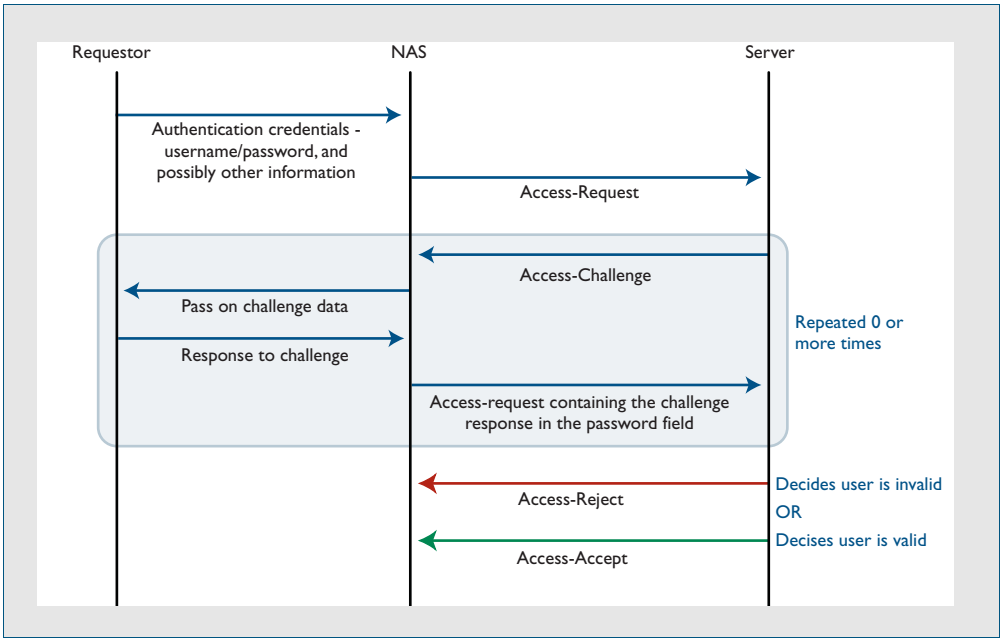
RADIUS Packets

The RADIUS RFCs define the RADIUS packet types and attributes. RADIUS authentication is defined by RFC2058, RFC2138, RFC2865, and RFC2868. RADIUS accounting is defined by RFC2059, RFC2139, RFC2866, and RFC2867. These RADIUS RFCs define over fifty attributes and six packets types (`Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, Access-Challenge`).

A RADIUS exchange is initiated by the NAS when a user requests access to the NAS. The NAS obtains the user authentication data adds them into a RADIUS `Access-Request` packet type and sends the RADIUS `Access-Request` packet to the RADIUS Server.

- If a RADIUS Server has not been configured for authentication request from a NAS then it will silently discard an `Access-Request` packet from it.
- If the RADIUS Server accepts the request from the NAS it considers the authentication date provided in the `Access-Request` packet. The RADIUS Server may verify the user from its own database or it may connect to other servers to verify.
- If the RADIUS Server decides that the user is not allowed access to the NAS it responds to the NAS with an `Access-Reject` packet and the NAS will block the user.
- If the RADIUS Server decides that the user is valid but needs more information to verify that the user is not an impostor, it may send an `Access-Challenge` packet to the NAS that the NAS forwards to the user. The NAS forwards the user response to the `Access-Challenge` packet in an `Access-Request` packet to the RADIUS Server to accept or reject to allow or deny NAS user access.
- If the RADIUS Server rejects the user it sends an `Access-Reject` packet to the NAS.
- If the RADIUS Server accepts the user it sends an `Accept-Accept` packet to the NAS. The `Accept-Accept` packet to the NAS contains attributes that the NAS can apply.

Figure 48-2: Example showing an exchange from a requestor to a NAS to a RADIUS server



RADIUS Attributes

Each attribute is identified by its RFC-defined name, followed by its attribute ID in parenthesis.

- **User-name(1)**

  User-names are strings of at least three characters and have a maximum of 253 characters, which is the upper limit on all RADIUS attributes.

- **User-password(2)**

  User-passwords are encrypted using an MD5 hash of the password, the NAS's shared secret with the RADIUS Server, and a request authenticator value. User-passwords can either be used at the initial authentication attempt or in response to an Access-Challenge packet type from the RADIUS Server to the NAS.

- **CHAP-password(3)**

  CHAP-passwords are used if the NAS is using CHAP to authenticate the user, and doesn't receive the use the user's password but sends the CHAP response to the RADIUS Server instead. The CHAP password is an encrypted string that is an MD5 hash of the password and challenge value sent by the user.

- **Framed-IP-Address(8)**

  Used for dial-in user making PPP connections to the NAS who are dynamically allocated an IP address that they can use for the duration of their connect. The RADIUS Server sends the Framed-IP-Address to the NAS to allocate.

- **Service-Type(6)**

  Used when the NAS is authenticating a user who wants to open a management session on the NAS, and is sent by the RADIUS Server back to the NAS in an Access-Accept type packet to indicate the level of access the NAS gives a user. Service-Type(6) is mapped to a Privileged management session for AlliedWare Plus.

- **NAS-Port-Type(61)**

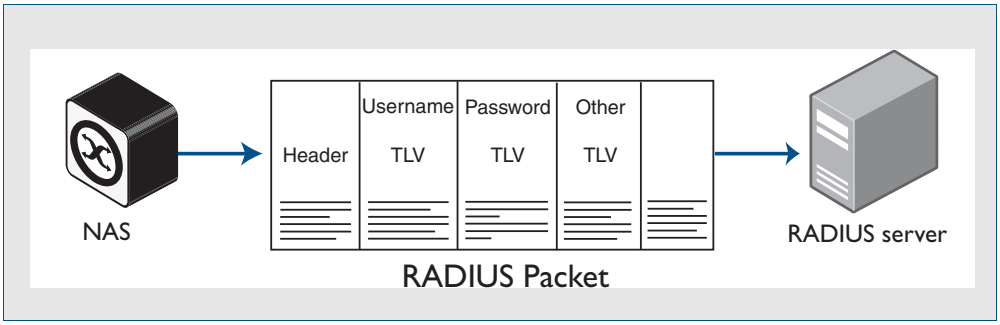
Identifies the type of port on which the user is accessing the NAS. The NAS-Port-Type(61) attribute is sent by the NAS to the RADIUS Server in Access-Request type packet, so the RADIUS Server may use it to choose access type. For 802.1X sessions, the NAS-Port-Type sent by the NAS is Ethernet (15).

- **802.1X VLAN assignment uses:**

  Tunnel-Type(64), Tunnel-Medium-Type(65), Tunnel-Private-Group-ID(81), Egress-VLANID(56), and Egress-VLAN-Name(58) attributes (specified in RFC4675 used to specify 802.1Q tagged and untagged VLAN assignments with LLDP-MED/Voice-VLAN).

Attributes are carried within RADIUS packets in the form of TLVs (Type Length Values). Every attribute has an attribute ID number in the Type field of the TLV. The Length field holds a one-byte number that represents then length of the TLV. The Value field holds the value of the attribute.

Figure 48-3: Example showing TLVs in a RADIUS packet from a NAS to a RADIUS server



RADIUS Security

RADIUS is used for network security and carries user authentication information, so can be a target for security attacks. To counter threats there are three elements to RADIUS security:

- **Shared secret**
- **Authenticator**
- **Password Encryption**

Shared secret

Every NAS and server are configured with a pre-shared key, called the “shared secret”, which is a key string, with no particular format of at least 16 characters.

The protocol has no method for choosing and sharing the secret between the NAS and the server. The secret must be manually generated and separately configured on the NAS and on the server.

The shared secret itself never appears in any RADIUS packets. It is used as an input to the algorithms used for creating encrypted values that are carried in the packets.

Authenticator

The authenticator is a random 16-byte value generated by the NAS. The NAS creates a new authenticator value for each `Access-Request` that it sends.

The response packets that come back from the server contain a value called the Response Authenticator. This is a value that is created by performing an MD5 hash on a string that is created by concatenating the packet type identifier, Session ID, Authenticator sent in the request packet, Attribute fields in the packet, Shared secret that the server shares with the NAS to which it is responding.

When the NAS receives the response packet, it performs the same hash on the same values, and verifies that it comes up with the same result. If not, then it must assume that the response packet has been spoofed, and silently discards it.

Password encryption

The value placed in the user-password TLV of an `Access-Request` packet is not simply an exact copy of the password sent from the requestor to the NAS.

The NAS concatenates together the shared secret and the authenticator that it has randomly generated for this request and then performs manipulations (MD5, XOR) on that concatenation, and the password to create the value to go into password TLV.

When the server validates the `Access-Request`, it retrieves the user's password from the user credentials database, and performs the same manipulation upon that password. If the result matches the value in the user-password field of the `Access-Request`, then the password sent by the requestor is deemed to be correct.

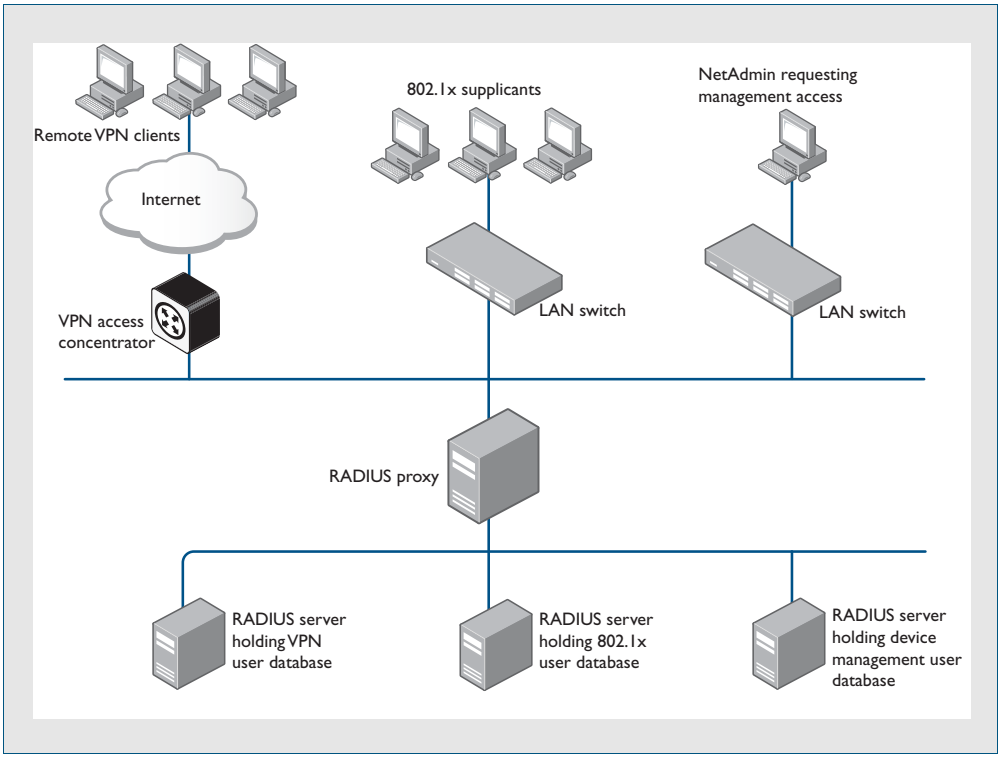
RADIUS Proxy

The user database, which user credentials sent to a RADIUS server are looked up in, may not reside on the RADIUS server itself. The external user database may reside on another RADIUS server, and the communication to that server uses RADIUS. In the case where a RADIUS server communicates with a NAS, but also acts as a client to another RADIUS server, is said to be acting as a RADIUS proxy.

There are a variety of situations where RADIUS proxy is useful. Multiple RADIUS servers could have been set up, holding user databases for different purposes such as Authentication, Switch management sessions, Authenticating VPN connections, and Authenticating 802.1X sessions.

But it is convenient for there to be just one address that all the NASs in the network use as their RADIUS server. That one RADIUS server that the NASs send their requests to, can act as a proxy for all the servers holding the different user databases.

Figure 48-4: Example showing RADIUS proxy



RADIUS Accounting

There are only two types of RADIUS accounting packet: `Accounting-Request` and `Accounting-Response`.

The `Accounting-Request` packets are always sent from the NAS to the server. The `Accounting-Response` packets are always sent from the server to the NAS, and are effectively ACKs of the `Accounting-Request` packets.

The `Accounting-Request` packets always carry the attribute `Acct-Status-Type`. The most commonly used values of this attribute are:

- **Start** – which denotes a packet marking that a session is beginning
- **Stop** – which denotes a packet marking that a session is ending
- **Interim update** – packets sent periodically during the session to give update reports on the statistics that are being collected.

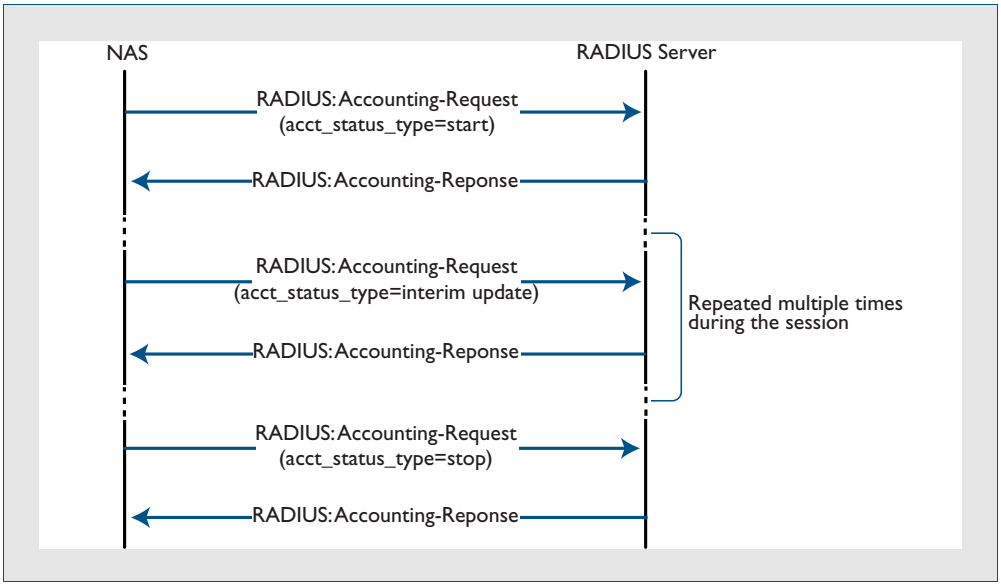
The statistics that can be exchanged in the session are:

- **Input Octets**
- **Input Packets**
- **Output Octets**
- **Output Packets**
- **Session Duration**

There is no requirement to exchange all these statistics – NAS implementations are at liberty to choose which statistics they will send. Each of these statistics has a corresponding attribute type. The attributes are sent in Interim-Update and Stop accounting request packets.

Each accounting session has a unique session ID, which is chosen by the NAS. The session ID is carried in an `Acct-Session-Id` attribute, that should be present in every packet involved in the session. The accounting packets typically do not use the same UDP port as the authentication packets. The default port for RADIUS accounting is 1813.

Figure 48-5: Example showing RADIUS accounting between a NAS and a RADIUS server



RADIUS Configuration

This section describes how to configure RADIUS with the available AAA commands. For a description of AAA commands, refer to the **AAA Commands** chapter. For a description of the RADIUS commands used, refer to the **RADIUS Commands** chapter.

RADIUS is often used in a variety of networks that need high security while maintaining access for remote users. RADIUS is suitable for the following networks that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database.
- Networks in which a user may access a single service. Using RADIUS, you can control user access to a single host, or to a single utility such as Telnet.
- Networks that require accounting. You can use RADIUS accounting independent of RADIUS authentication. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (time, packets, bytes) used.

Switch Configuration Tasks

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the **aaa authentication** command to define method lists for RADIUS authentication. For information about this command, refer to the **AAA Commands** chapter.
- Use authentication commands to enable the defined method lists to be used. For more information, refer to the **Authentication Commands** chapter.

The following configuration tasks are optional:

- You can use the **aaa group server** command to group selected RADIUS hosts for specific services. For detailed information about this command, refer to the **AAA Server Groups Configuration** section in this chapter and refer to the **AAA Commands** chapter.
- You can use the **aaa accounting login** command to enable accounting for RADIUS connections. For information about this command, refer to the **AAA Commands** chapter.

This section describes how to set up RADIUS for authentication and accounting on your network, and includes the following sections:

- Switch to RADIUS Server Communication (Required)
- Configuring AAA Server Groups (Optional)
- Configuring AAA Server Groups with Deadtime (Optional)
- Specifying RADIUS Authentication
- Specifying RADIUS Accounting (Optional)

For RADIUS configuration examples using the commands in this chapter, refer to the section **RADIUS Configuration Examples** at the end of this chapter.

Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from a software provider. Switch to RADIUS server communication has several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

A RADIUS server and a switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS using the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text string that it shares with the switch, which you can specify using the **key** parameter in the **radius-server host** command.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch, use the three global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** command.

Note

You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Network Access Server.

If both global and per-server functions are configured on a switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

To configure per-server RADIUS server communication, use the following command in the Global Configuration mode:

Mode and Command	Command Purpose
awplus(config)# radius-server host {<*hostname*>| <*ip-address*>} [auth-port <*port-number*>] [acct-port <*port-number*>] [timeout <*seconds*>] [retransmit <*retries*>] [key <*string*>]	Specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers. Use the `auth-port <port-number>` option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the `acct-port <port-number>` option to configure a specific UDP port on this RADIUS server to be used solely for accounting. To configure the network access server to recognize more than one host entry associated with a single IP address, simply repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host. If no timeout is set, the global value is used; otherwise, enter a value in the range 1 to 1000. If no retransmit value is set, the global value is used; otherwise enter a value in the range 1 to 1000. If no key string is specified, the global value is used.

To configure global communication settings between the switch and a RADIUS server, use the following **radius-server** commands in the Global Configuration mode:

Mode and Command	Command Purpose
awplus(config)# radius-server key <*key*>	Specifies the shared secret text string used between the switch and a RADIUS server (no default is set).
awplus(config)# radius-server retransmit <*retries*>	Specifies how many times the switch transmits each RADIUS request to the RADIUS server before giving up (the default is 3).
awplus(config)# radius-server timeout <*seconds*>	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
awplus(config)# radius-server deadtime <*minutes*>	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

AAA Server Groups Configuration

Configuring the switch to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service.

To define a server host with a server group name, enter the following commands in the Global Configuration mode. The listed RADIUS server must exist in the Global Configuration mode:

Mode and Command	Command Purpose
awplus(config)# radius-server host {*<hostname>*| *<ip-address>*} [auth-port *<port-number>*] [acct-port *<port-number>*] [timeout *<seconds>*] [retransmit *<retries>*] [key *<string>*]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the section **Switch to RADIUS Server Communication** of this chapter for more information on the **radius-server host** command.
awplus(config-if)# aaa group server *<group-name>*	Defines the AAA server group with a group name. This command puts the switch in server group sub configuration mode.
awplus(config-sg)# server {*<hostname>*|*<ip-address>*} [auth-port *<port-number>*] [acct-port *<port-number>*]	Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be defined previously using the radius-server host command.

Configuring AAA server groups with deadtime

After you have configured a server host with a server name, you can use the **deadtime (RADIUS server group)** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring **deadtime** is no longer limited to a global configuration. A separate timer has been attached to each server host in every server group. When a server is found to be unresponsive after numerous retransmissions and time-outs, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server, once it is assumed to be dead, are directed to alternate servers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers, if running, for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note Since one server has different timers and may have different deadtime values configured in the server groups, the same server may in the future have different states, dead and alive, at the same time. To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

To configure deadtime within a server group, use the following commands beginning in the Global Configuration mode:

Mode and Command	Command Purpose
`awplus(config)#` `aaa group server radius group1`	Defines a RADIUS type server group.
`awplus(config-sg)#` `deadtime 1`	Configures and defines a deadtime value in minutes.
`awplus(config-sg)#` `exit`	Exits server group configuration mode.

Specifying RADIUS authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication login** command, specifying RADIUS as the authentication method. For detailed **aaa authentication login** command information, refer to the **AAA Commands** chapter.

Specifying RADIUS accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the **aaa accounting login** command, specifying RADIUS as the accounting method. For detailed **aaa accounting login** command information, refer to the **AAA Commands** chapter.

Monitoring and maintaining RADIUS

To monitor and maintain RADIUS, use the following commands in Privileged Exec mode:

Mode and Command	Command Purpose
`awplus#` `debug radius`	Displays information associated with RADIUS. For detailed **debug radius** command information, refer to the **RADIUS Commands** chapter.
`awplus#` `show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets. For detailed **show radius statistics** command information, refer to the **RADIUS Commands** chapter.

RADIUS Configuration Examples

The following sections provide RADIUS configuration examples:

- RADIUS Authentication
- Single RADIUS Server Configuration
- Multiple RADIUS Server Configuration
- RADIUS Server Group Configuration
- RADIUS Server Configuration using Server Groups

RADIUS Authentication

Example The following example shows how to configure the switch to authenticate using RADIUS.

Figure 48-6: Sample RADIUS authentication to configure the switch to authenticate users

```
!
radius-server host 172.10.10.1
radius-server key radiuspass
username newuser password newpass
aaa authentication login admin
!
```

The lines in this example RADIUS authentication and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication login** command defines a method list named **admin** for login authentication.

Example The following example shows how to configure the switch to authenticate logins using RADIUS.

Figure 48-7: Sample RADIUS authentication to authenticate logins

```
!
aaa authentication login radius-login group radius
!
```

This sample RADIUS authentication configuration is defined as follows:

- The **aaa authentication login radius-login group radius** command configures the switch to use RADIUS for authentication at the login prompt.

Example The following example shows how to configure the authentication method to verify a username and password at login. In this example, if a username is entered at the username prompt, that username is used for authentication.

Figure 48-8: Sample RADIUS authentication to verify a username and password

```
!
aaa authentication login default group radius
radius-server host 172.10.10.1 auth-port 1812 acct-port 1813
!
```

The lines in this sample RADIUS authentication configuration are defined as follows:

- The **aaa authentication login default group radius** command specifies that the username and password are verified by RADIUS.
- The **radius-server host 172.10.10.1 auth-port 1812 acct-port 1813** command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.

Single RADIUS Server Configuration

Example The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.2.2.2.

Figure 48-9: Single RADIUS server sample configuration

```
!
radius-server host 172.2.2.2 timeout 5 retransmit 5 key 10
!
```

Multiple RADIUS Server Configuration

Example The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses `172.2.2.2` and `172.1.1.1`

Figure 48-10: Multiple RADIUS server sample configuration

```
!
! Enable and configure radius authentication and accounting
! services on the switch:
!
aaa authentication login default group radius
aaa accounting default start-stop group radius
!
! Change the retransmission value for all RADIUS servers:
!
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and
! key values. Change the default auth-port and acct-port
! values.
!
radius-server host 172.2.2.2 auth-port 1645 acct-port 1646
timeout 3 retransmit 3 key radkey
!
! Configure per-server specific timeout and key values. This
! server uses the global retransmission value.
!
radius-server host 172.1.1.1 timeout 6 key rad123
!
```

RADIUS Server Group Configuration

Example The following example shows how to create server group `group2` with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports.

Figure 48-11: RADIUS server group sample configuration using the same IP address

```
!
aaa group server radius group2
  server 172.1.1.1 auth-port 1645 acct-port 1646
  server 172.1.1.1 auth-port 1812 acct-port 1813
  server 172.1.1.1 auth-port 2000 acct-port 2001
!
```

RADIUS Server Configuration using Server Groups

The following example shows how to configure the network access server to recognize two different RADIUS server groups.

One of these groups, `group1`, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as fail over backup to the first one. Each group is individually configured for `deadtime`; `deadtime` for `group1` is one minute, and `deadtime` for `group2` is two minutes.

Figure 48-12: Multiple RADIUS servers using server groups sample configuration

```
!
! The following command configures default RADIUS parameters:
!
aaa authentication login default group group1
!
! The following commands define the group1 RADIUS server group
! and associate servers with it and configures a deadtime of
! one minute:
!
aaa group server radius group1
  server 172.1.1.1 auth-port 1645 acct-port 1646
  server 172.2.2.2 auth-port 1812 acct-port 1813
  deadtime 1
!
! The following commands define the group2 RADIUS server group
! and associate servers with it and configures a deadtime of
! two minutes:
!
aaa group server radius group2
  server 172.2.2.2 auth-port 1812 acct-port 1813
  server 172.3.3.3 auth-port 2000 acct-port 2001
  deadtime 2
!
! The following commands configure the RADIUS attributes
! for each host entry associated with one of the defined
! server groups:
!
radius-server host 172.1.1.1 auth-port 1645 acct-port 1646
radius-server host 172.2.2.2 auth-port 1812 acct-port 1813
radius-server host 172.3.3.3 auth-port 2000 acct-port 2001
!
```

Chapter 49: RADIUS Commands

Command List 49.2
deadtime (RADIUS server group) 49.2
debug radius 49.3
ip radius source-interface 49.4
radius-server deadtime 49.5
radius-server host 49.6
radius-server key 49.10
radius-server retransmit 49.11
radius-server timeout 49.12
server (Server Group) 49.14
show debugging radius 49.16
show radius 49.17
show radius statistics 49.19
undebug radius 49.19

Command List

This chapter provides an alphabetical reference for commands used to configure the device to use RADIUS servers.

deadtime (RADIUS 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 on page 49.5. The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is "dead". Note that a RADIUS server is considered "dead" if there is no response from the server within a defined time period.

Use the **no** variant of this command to reset the deadtime configured for the RADIUS server group. If the global deadtime for RADIUS server is configured the value will be used for the servers in the group. The global deadtime for the RADIUS server is set to 0 minutes by default.

Syntax

```
deadtime <0-1440>
no deadtime
```

Parameter	Description
<0-1440>	Amount of time in minutes.

Default The deadtime is set to 0 minutes by default.

Mode Server Group Configuration

Usage If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked "dead", and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

Examples To configure the deadtime for 5 minutes for the RADIUS server group "GROUP1", use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group "GROUP1", use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

Related Commands **aaa group server**
radius-server deadtime

debug radius

This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

Syntax

```
debug radius [packet|event|all]
no debug radius [packet|event|all]
```

Parameter	Description
`packet`	Debugging for RADIUS packets is enabled or disabled.
`event`	Debugging for RADIUS events is enabled or disabled.
`all`	Enable or disable all debugging options.

Default RADIUS debugging is disabled by default.

Mode Privileged Exec

Examples To enable debugging for RADIUS packets, use the command:

```
awplus#  debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus#  debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

Related Commands **show debugging radius**
undebug radius

ip radius source-interface

This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

Syntax

```
ip radius source-interface {<interface>|<ip-address>}
no ip radius source-interface
```

Parameter	Description
<interface>	Interface name.
<ip-address>	IP address in the dotted decimal format A.B.C.D.

Default Source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Mode Global Configuration

Examples To configure all outgoing RADIUS packets to use the IP address of the interface “vlan1” for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface vlan1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

Related Commands **radius-server host**
show radius statistics

radius-server deadtime

Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

Syntax

```
radius-server deadtime <minutes>
no radius-server deadtime
```

Parameter	Description
<minutes>	RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).

Default The default RADIUS deadtime configured on the system is 0 seconds.

Mode Global Configuration

Usage The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the **radius-server retransmit** command or for the server by the **radius-server host** command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

Examples To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

Related Commands

deadtime (RADIUS server group)
radius-server host
radius-server retransmit
show radius statistics

radius-server host

Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax

```
radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>]
   [auth-port <0-65535>] [key <key-string>] [retransmit <0-100>]
   [timeout <1-1000>]

no radius-server host {<host-name>|<ip-address>}
   [acct-port <0-65535>] [auth-port <0-65535>]
```

Parameter	Description
<host-name>	Server host name. The DNS name of the RADIUS server host.
<ip-address>	The IP address of the RADIUS server host.
acct-port	Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.
<0-65535>	UDP port number (Accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting.
auth-port	Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.
<0-65535>	UDP port number (Authentication port number is set to 1812 by default) Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.

Parameter(cont.)	Description(cont.)
`timeout`	Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the **radius-server timeout** command is used.
<1-1000>	Time in seconds to wait for a server reply (timeout is set to 5 seconds by default) The time interval (in seconds) to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the **radius-server timeout** command. If no timeout value is specified for this server, the global value is used.
`retransmit`	Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the **radius-server retransmit** command is used.
<0-100>	Maximum number of retries (maximum number of retries is set to 3 by default) The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used.
`key`	Set shared secret key with RADIUS servers
<key-string>	Shared key string applied Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the string are used. If spaces are used in the string, do not enclose the string in quotation marks unless the quotation marks themselves are part of the key. This setting overrides the global setting of the **radius-server key c**ommand. If no key value is specified, the global value is used.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius-server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the auth-port parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to **allied** on the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key allied
```

To delete the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure `rad1.company.com` for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com
                acct-port 0
```

To remove the RADIUS server `rad1.company.com` configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com
                acct-port 0
```

To configure `rad2.company.com` for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com
                auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal

awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Related Commands

aaa group server
radius-server key
radius-server retransmit
radius-server timeout
show radius statistics

radius-server key

This command sets a global secret key for RADIUS authentication on the switch. The shared secret text string is used for RADIUS authentication between the switch and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

Syntax

```
radius-server key <key>
no radius-server key
```

Parameter	Description
<key>	Shared secret among radius server and 802.1X client.

Default The RADIUS server secret key on the system is not set by default (null).

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its RADIUS servers. If no secret key is specified for a particular RADIUS server using the **radius-server host** command, this global key is used.

After enabling AAA authentication with the **aaa authentication login** command, set the authentication and encryption key using the **radius-server key** command so the key entered matches the key used on the RADIUS server.

Examples To set the global secret key to **allied** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key allied
```

To set the global secret key to **secret** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key secret
```

To delete the global secret key for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server key
```

Related Commands **radius-server host**
show radius statistics

radius-server retransmit

This command sets the retransmit counter to use RADIUS authentication on the switch. This command specifies how many times the switch transmits each RADIUS request to the RADIUS server before giving up.

This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.

Use the **no** variant of this command to reset the re-transmit counter to the default (3).

Syntax

```
radius-server retransmit <retries>
no radius-server retransmit
```

Parameter	Description
<retries>	RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the **radius-server host** command, this global value is used.

Default The default RADIUS retransmit count on the switch is 3.

Mode Global Configuration

Examples To set the RADIUS **retransmit** count to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 1
```

To set the RADIUS **retransmit** count to the default (3), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server retransmit
```

To configure the RADIUS **retransmit** count globally with 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 5
```

To disable retransmission of requests to a RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 0
```

Related Commands

radius-server deadtime
radius-server host
show radius statistics

radius-server timeout

Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

Parameter	Description
<seconds>	RADIUS server timeout in seconds in the range 1 to 1000. The global time in seconds to wait for a RADIUS server to reply to a request before retransmitting the request, or considering the server to be dead (depending on the **radius-server retransmit** command).

Default The default RADIUS transmit timeout on the system is 5 seconds.

Mode Global Configuration

Examples To globally set the device to wait 20 seconds before retransmitting a RADIUS request to unresponsive RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 20
```

To set the RADIUS **timeout** parameter to 1 second, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 1
```

To set the RADIUS **timeout** parameter to the default (5 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

To configure the RADIUS server **timeout** period globally with 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 3
```

To reset the global **timeout** period for RADIUS servers to the default, use the following command:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

Related Commands

radius-server deadtime
radius-server host
radius-server retransmit
show radius statistics

server (Server Group)

This command adds a RADIUS server to a server group in Server-Group Configuration mode. The RADIUS server should be configured by the **radius-server host** command.

The server is appended to the server list of the group and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before added as a new server.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set `auth-port` to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set `acct-port` to 0. If the accounting port is missing, the default port number is 1812.

Use the **no** variant of this command to remove a RADIUS server from the server group.

Syntax

```
server {<hostname>|<ip-address>}
    [auth-port <0-65535>][acct-port <0-65535>]

no server {<hostname>|<ip-address>}
    [auth-port <0-65535>][acct-port <0-65535>]
```

Parameter	Description
<hostname>	Server host name
<ip-address>	Server IP address The server is identified by IP address, authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports.
`auth-port`	Authentication port The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set **auth-port** to 0. If the authentication port is missing, the default port number is 1812.
<0-65535>	UDP port number (default: 1812)
`acct-port`	Accounting port The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set **acct-port** to 0. If the accounting port is missing, the default port number is 1813.
<0-65535>	UDP port number (default: 1813)

Default The default Authentication port number is 1812 and the default Accounting port number is 1813.

Mode Server Group Configuration

Usage The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the **auth-port** and **acct-port** parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

Examples To create a RADIUS server group RAD_AUTH1 for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000
acct-port 0
```

To create a RADIUS server group RAD_ACCT1 for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0
acct-port 1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group **GROUP1**, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

Related Commands
aaa accounting auth-mac default
aaa accounting auth-web default
aaa accounting dot1x
aaa accounting login
aaa authentication auth-mac
aaa authentication auth-web
aaa authentication login
aaa group server
radius-server host

show debugging radius

This command displays the current debugging status for the RADIUS servers.

Syntax `show debugging radius`

Mode User Exec and Privileged Exec

Example To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

Output **Figure 49-1: Example output from the show debugging radius command**

```
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`

Mode User Exec and Privileged Exec

Example To display the current status of RADIUS servers, use the command:

```
awplus# show radius
```

Output **Figure 49-2: Example output from the show radius command showing RADIUS servers**

```
RADIUS Global Configuration
Source Interface : not configured
Secret Key : secret
Timeout : 5 sec
Retransmit Count : 3
Deadtime : 20 min
Server Host : 192.168.1.10
Authentication Port : 1812
Accounting Port : 1813
Secret Key : secret
Timeout : 3 sec
Retransmit Count : 2
Server Host : 192.168.1.11
Authentication Port : 1812
Accounting Port : not configured
Server Name/Auth Acct Auth Acct
IP Address Port Port Status Status
-------------------------------------------------------------
192.168.1.10 1812 1813 Alive Alive
192.168.1.11 1812 N/A Alive N/A
```

Example See the sample output below showing RADIUS client status and RADIUS configuration:

```
awplus# show radius
```

Output **Figure 49-3: Example output from the show radius command showing RADIUS client status**

```
RADIUS global interface name: awplus
Secret key:
Timeout: 5
Retransmit count: 3
Deadtime: 0

Server Address: 150.87.18.89
Auth destination port: 1812
Accounting port: 1813
Secret key: swg
Timeout: 5
Retransmit count: 3
Deadtime: 0show radius local-server group
```

Output Parameter	Meaning	
`Source Interface`	The interface name or IP address to be used for the source address of all outgoing RADIUS packets.	
`Secret Key`	A shared secret key to a radius server.	
`Timeout`	A time interval in seconds.	
`Retransmit Count`	The number of retry count if a RADIUS server does not response.	
`Deadtime`	A time interval in minutes to mark a RADIUS server as “dead”.	
`Interim-Update`	A time interval in minutes to send Interim-Update Accounting report.	
`Group Deadtime`	The deadtime configured for RADIUS servers within a server group.	
`Server Host`	The RADIUS server hostname or IP address.	
`Authentication Port`	The destination UDP port for RADIUS authentication requests.	
`Accounting Port`	The destination UDP port for RADIUS accounting requests.	
`Auth Status`	The status of the authentication port. The status (“dead”, “error”, or “alive”) of the RADIUS authentication server and, if dead, how long it has been dead for.	
	`Alive`	The server is alive.
	`Error`	The server is not responding.
	`Dead`	The server is detected as dead and it will not be used for deadtime period. The time displayed in the output shows the server is in dead status for that amount of time.
	`Unknown`	The server is never used or the status is unknown.
`Acct Status`	The status of the accounting port. The status (“dead”, “error”, or “alive”) of the RADIUS accounting server and, if dead, how long it has been dead for.	

show radius statistics

This command shows the RADIUS client statistics for the switch.

Syntax `show radius statistics`

Mode User Exec and Privileged Exec

Example See the sample output below showing RADIUS client statistics and RADIUS configuration:

```
awplus# show radius statistics
```

Output **Figure 49-4: Example output from the show radius statistics command:**

```
RADIUS statistics for Server: 150.87.18.89
Access-Request Tx : 5 - Retransmit : 0
Access-Accept Rx : 1 - Access-Reject Rx : 2
Access-Challenge Rx : 2
Unknown Type : 0 - Bad Authenticator: 0
Malformed Access-Resp: 0 - Wrong Identifier: 0
Bad Attribute : 0 - Packet Dropped : 0
TimeOut : 0 - Dead count : 0
Pending Request: 0
```

undebug radius

This command applies the functionality of the **no debug radius** command on page 49.3.

Chapter 50: TACACS+ Introduction and Configuration

Introduction 50.2
TACACS+ Overview 50.2
The AlliedWare Plus TACACS+ Implementation 50.2
Authentication 50.3
Authorization 50.3
Accounting 50.4
Configuration 50.5
Configure TACACS+ 50.5
TACACS+ Configuration Example 50.7

Introduction

This chapter provides information about the AlliedWare Plus implementation of TACACS+ and how to configure it on this switch. For detailed descriptions of the commands used to configure TACACS+, see **Chapter 51, TACACS+ Commands**. For information about Authentication, Authorization and Accounting (AAA), see **Chapter 44, AAA Introduction and Configuration** and **Chapter 45, AAA Commands**.

TACACS+ Overview

TACACS+ (Terminal Access Controller Access-Control System Plus) provides a method for securely managing multiple network access points from a single management service.

TACACS+ is a TCP-based access control protocol, utilizing TCP port 49, that allows a device to forward a user's username and password to an authentication server to determine whether access can be allowed. In addition to this authentication service, TACACS+ can also provide authorization and accounting services.

One of the features of TACACS+ is the ability to separate authentication, authorization and accounting so that these functions can be provided independently on separate servers. Authentication involves identifying a user, typically by requiring the user to supply a valid username and password before access is granted. Following authentication, the user must gain authorization to perform tasks. For example, after logging into a switch, a user may try to issue configuration commands. The authorization process determines whether the user has the authority to issue these commands. Authorization is always preceded by authentication.

The AlliedWare Plus TACACS+ Implementation

The AlliedWare Plus TACACS+ implementation provides authentication, authorization, and accounting. Note that:

- Authorization cannot be performed independently of the authentication process. There are no authorization commands available.
- Authentication and authorization must be configured on the same server.
- Authorization is only applicable if enable password authentication has not been configured with the **aaa authentication enable default group tacacs+** command.

With the AlliedWare Plus TACACS+ implementation, all traffic that passes between the TACACS+ client and the TACACS+ servers on the network is encrypted. TACACS+ encrypts the entire payload of packets, which means that it encrypts the user's password between the client and the server.

A TACACS+ client is available on your switch. You need a system running TACACS+ server software from a software provider to use the TACACS+ functionality on your switch.

Authentication

The TACACS+ protocol can forward many types of username and password information. The AlliedWare Plus TACACS+ implementation supports username and password login authentication, as well as enable password authentication. This information is encrypted over the network with MD5 (Message Digest 5).

When TACACS+ login authentication is enabled on the switch with the **aaa authentication login** command and at least one TACACS+ server is configured and reachable, all user login authentications are authenticated against the TACACS+ server. No local login or other means of authentication is allowed or accepted by the switch unless the switch has been configured to use another authentication method as a backup, and the TACACS+ server is not reachable.

When TACACS+ enable password authentication is enabled on the switch with the **aaa authentication enable default group tacacs+** command and at least one TACACS+ server is configured and reachable, all user attempts to access a higher privilege level using the **enable (Privileged Exec mode)** command are authenticated against the TACACS+ server. If TACACS+ enable password authentication is enabled and the TACACS+ server is not reachable, then the user is only granted access to the desired privilege level if a backup authentication method is also configured.

Note

If TACACS+ login authentication is enabled on the switch, and enable password authentication is configured as default with the **aaa authentication enable default local** command, then a local enable password must be configured for each privilege level that needs to be accessible to users.

Authorization

In the AlliedWare Plus TACACS+ implementation, authorization cannot be performed independently of the authentication process. Authorization is concerned with what users are allowed to do once they have gained access to the managed device. This involves the passing of Attribute Value pairs (AV pairs) from the TACACS+ server to the managed device. An AV pair is made up of two pieces of information: the attribute that identifies the parameter to be set, and the value that specifies the value to assign to that parameter. These AV pairs are configured on a per-user or per-group basis on the TACACS+ server. The AV pairs that are supported by the AlliedWare Plus TACACS+ implementation are:

- **Privilege Level**

  Privilege levels range from 1 to 15, with 15 being the highest. For information about privilege levels see **"How to Add and Remove Users" on page 1.27** and the **username** command on page 5.37.

- **Timeout**

  The value assigned to this attribute specifies the length of time that the session can exist. After this value has expired, the session will either be disconnected, or have the privilege of the user reduced. The valid range of timeout values is 0 to 65535 (minutes).

- **Idletime**

  If no input or output traffic is received or sent in the period specified by the value for this attribute, the session is disconnected. The valid idletime range is 0 to 65535 (minutes).

Note

In the AlliedWare Plus TACACS+ implementation, authorization for privilege level, timeout, and idletime AV pairs is only attempted if enable password authentication (**aaa authentication enable default group tacacs+** command) is not configured. If enable password authentication is configured then the privilege level a user is granted access to is determined during the enable password authentication session.

Accounting

TACACS+ accounting usually takes place after authentication and authorization. However, because TACACS+ separates these three functions, neither authentication nor authorization are required for accounting to function. TACACS+ accounting provides the following two distinct functions:

- a record of services used for billing purposes
- an audit trail for user exec sessions

The AlliedWare Plus TACACS+ accounting implementation supports an audit trail for user exec sessions only. This includes the ability to configure accounting for user logins and logouts, and accounting of any commands executed by the user while they are logged into the switch.

TACACS+ accounting includes three different types of accounting records:

- **start** records that indicate a service is about to start
- **stop** records that indicate a service has just ended
- **update** records that indicate a service is still in progress

Configuration

This section describes how to set up TACACS+ for login authentication, enable password authentication, and accounting.

The TACACS+ server is normally a multiuser system running TACACS+ server software from a software provider. TACACS+ servers are identified on the basis of their host name or IP address. A TACACS+ server and a switch use a shared secret text string to encrypt passwords and exchange responses. To configure TACACS+, you must specify the host running the TACACS+ server software and a secret text string that it shares with the switch.

Configure TACACS+

Table 50-1: General configuration procedure for TACACS+ authentication and accounting

Step 1. Specify a remote TACACS+ server and the shared secret key	
`awplus#`	
`configure terminal`	Enter Global Configuration mode.
`awplus(config)#`	
`tacacs-server host {<host-name>|<ip-address>} [key [8]<key-string>]`	Specify the IP address or host name of the remote TACACS+ server host and the shared secret key to use with the specified TACACS+ server. Specify 8 if you are entering a password as a string that has already been encrypted instead of entering a plain text password. As many as four TACACS+ servers can be configured and consulted for authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn.
`awplus(config)#`	
`tacacs-server key [8] <key-string>`	Specify the global shared secret text string used between the switch and **all** TACACS+ servers. Specify `8` if you are entering a password as a string that has already been encrypted instead of entering a plain text password. If no secret key is explicitly specified for a TACACS+ server with the **tacacs-server host** command, the global secret key will be used.
Step 2. Specify the timeout value	
`awplus(config)#`	
`tacacs-server timeout <seconds>`	Specify for how many seconds a switch waits for a reply to a TACACS+ request before considering the TACACS+ server dead.

Table 50-1: General configuration procedure for TACACS+ authentication and accounting(cont.)

Step 3. Define the method list for TACACS+ login authentication	
`awplus(config)#`	
`aaa authentication login {default|<list-name>} {[local] [group {radius|tacacs+|<group-name>}]}`	This method list defines the AAA server type used for login authentication. The server types are always used in the order specified with this command. If the first server in the method list is unreachable, the switch sends the request to the next server in the list. If the authentication server denies the authentication request because of an incorrect username or password then the user login fails.
Step 4. Define the method list for TACACS+ enable password authentication	
`awplus(config)#`	
`aaa authentication enable default group tacacs+ [local] [none]`	This method list defines the authentication method used to determine the privilege command level a user can access. Specify **local** to use the locally configured enable password and **none** to grant access to Privileged Exec mode with no authentication, if the TACACS+ server goes offline, or is not reachable during enable password authentication.
Step 5. Define the method for TACACS+ login accounting	
`awplus(config)#`	
`aaa accounting login {default|<list-name>} {start-stop|stop-only|none} {group {radius|tacacs+|<group-name>}}`	You can only define one method for login accounting, either RADIUS or TACACS+. Specify **start-stop** to send both start and stop login accounting records, **stop-only** to send only stop login accounting records, or **none** to disable the sending of login accounting records.
Step 6. Configure TACACS+ command accounting	
`awplus(config)#`	
`aaa accounting commands <1-15> default stop-only group tacacs+`	TACACS+ command accounting is configured per privilege level and only commands of the specified privilege level are accounted. Therefore, if you require that all commands are accounted to the TACACS+ server, you must configure command accounting for each privilege level separately. Commands are accounted to the TACACS+ server after they have successfully executed.
Step 7. Troubleshooting TACACS+	
`awplus(config)#`	
`show tacacs+`	Display the current TACACS+ server configuration and status.
`awplus#`	
`debug aaa authentication`	Enable debug output for TACACS+ authentication.
`awplus#`	
`debug aaa authorization`	Enable debug output for TACACS+ authorization.
`awplus#`	
`debug aaa accounting`	Enable debug output for TACACS+ accounting.

TACACS+ Configuration Example

Example The following example shows how to configure the switch to authenticate and account using TACACS+.

Figure 50-1: Sample TACACS+ authentication and accounting to configure the switch to authenticate and account user exec sessions

```
!
tacacs-server host 172.10.10.1
tacacs-server key tacacspass
aaa authentication login admin group tacacs+ local
aaa authentication enable default group tacacs+ local
aaa accounting login admin start-stop group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 7 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+

line console 0
login authentication admin
accounting login admin
!
```

The lines in this example TACACS+ authentication and accounting configuration are defined as follows:

- The **tacacs-server host** command defines the IP address of the TACACS+ server host.
- The **tacacs-server key** command defines the global shared secret text string between the network access server and the TACACS+ server host.
- The **aaa authentication login** command defines a method list named **admin** to use first the TACACS+ servers and then the local user database for user login authentication.
- The **aaa authentication enable default group tacacs+** command defines a method list to use first the TACACS+ servers and then the local enable passwords, set with the **enable password** command, for user enable password authentication.
- The **aaa accounting login** command defines a method named **admin** to use TACACS+ servers for login accounting.
- The **aaa accounting commands** command specifies the privilege level of the commands that will be accounted.
- The **login authentication** command specifies that this method list will be used for authenticating users logging in on the asynchronous console port.
- The **accounting login** command specifies that this method list will be used for accounting users logging in on the asynchronous console port.

Chapter 51: TACACS+ Commands

Command List 51.2
show tacacs+ 51.3
tacacs-server host 51.4
tacacs-server key 51.7
tacacs-server timeout 51.8

Command List

This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACAC+, see **Chapter 50, TACACS+ Introduction and Configuration**.

show tacacs+

This command displays the current TACACS+ server configuration and status.

Syntax `show tacacs+`

Mode User Exec and Privileged Exec

Example To display the current status of TACACS+ servers, use the command:

```
awplus# show tacacs+
```

Output **Figure 51-1: Example output from the show tacacs+ command**

```
TACACS+ Global Configuration
  Timeout              : 5 sec

Server Host/      Server
IP Address        Status
------------------------------------------------------------
192.168.1.10      Alive
192.168.1.11      Unknown
```

Table 51-1: Parameters in the output of the show tacacs+ command

Output Parameter	Meaning	
`Timeout`	A time interval in seconds.	
`Server Host/IP Address`	TACACS+ server hostname or IP address.	
`Server Status`	The status of the authentication port.	
	`Alive`	The server is alive.
	`Dead`	The server has timed out.
	`Error`	The server is not responding or there is an error in the key string entered.
	`Unknown`	The server is never used or the status is unkown.
	`Unreachable`	The server is unreachable.
	`Unresolved`	The server name can not be resolved.

tacacs-server host

Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

Syntax

```
tacacs-server host {<host-name>|<ip-address>} [key [8]<key-string>]
no tacacs-server host {<host-name>|<ip-address>}
```

Parameter	Description
<host-name>	Server host name. The DNS name of the TACACS+ server host.
<ip-address>	The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.
`key`	Set shared secret key with TACACS+ servers.

Parameter(cont.)	Description(cont.)
8	Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the **tacacs-server key** command. If no key value is specified, the global value is used.

Default No TACACS+ server is configured by default.

Mode Global Configuration

Usage A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable
- it cannot communicate with the switch properly due to the switch and the server having different secret keys

Examples To add the server `tac1.company.com` as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to `secret` on the TACACS+ server `192.168.1.1`, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server `tac1.company.com`, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

Related Commands

aaa accounting commands
aaa authentication login
tacacs-server key
tacacs-server timeout
show tacacs+

tacacs-server key

This command sets a global secret key for TACACS+ authentication, authorization and accounting. The shared secret text string is used for TACACS+ communications between the switch and all TACACS+ servers.

Note that if no secret key is explicitly specified for a TACACS+ server with the **tacacs-server host** command, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to remove the global secret key.

Syntax

```
tacacs-server key [8] <key-string>
no tacacs-server key
```

Parameter	Description
8	Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and all TACACS+ servers. This key must match the encryption used on the TACACS+ server.

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the **tacacs-server host** command, this global key is used.

Examples To set the global secret key to `secret` for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

Related Commands **tacacs-server host**
show tacacs+

tacacs-server timeout

Use this command to specify the TACACS+ global timeout value. The timeout value is how long the device waits for a reply to a TACACS+ request before considering the server to be dead.

Note that this command configures the **timeout** parameter for TACACS+ servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
tacacs-server timeout <seconds>
no tacacs-server timeout
```

Parameter	Description
<seconds>	TACACS+ server timeout in seconds, in the range 1 to 1000.

Default The default timeout value is 5 seconds.

Mode Global Configuration

Examples To set the timeout value to 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server timeout 3
```

To reset the timeout period for TACACS+ servers to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

Related Commands **tacacs-server host**
show tacacs+

Chapter 52: Secure Shell (SSH) Introduction

Introduction 52.2
Secure Shell on the AlliedWare Plus OS 52.2
Configuring the SSH Server 52.4
Creating a Host Key 52.4
Enabling the Server 52.4
Modifying the Server 52.5
Validating the Server Configuration 52.6
Adding SSH Users 52.6
Authenticating SSH Users 52.7
Adding a Login Banner 52.7
Monitoring the Server and Managing Sessions 52.8
Debugging the Server 52.8
Configuring the SSH Client 52.9
Modifying the Client 52.9
Adding SSH Servers 52.10
Authenticating with a Server 52.10
Connecting to a Server and Running Commands 52.11
Copying files to and from the Server 52.11
Debugging the Client 52.11

Introduction

This chapter describes how the Secure Shell protocol is implemented in the AlliedWare Plus™ Operating System. It covers:

- Support for Secure Shell.
- Configuring your device as a Secure Shell server and client.
- Using Secure Shell to manage your device.

The AlliedWare Plus™ OS supports SSH version 2 and SSH version 1.5, making it backwards compatible with SSH version 1.

Secure management is important in modern networks, as the ability to easily and effectively manage switches and routers, and the requirement for security, are two almost universal requirements. Protocols such as Telnet and rlogin allow you to manage devices remotely, but can have serious security problems, such as relying on reusable plaintext passwords that are vulnerable to wiretapping or password guessing. The Secure Shell (SSH) protocol is superior to these protocols by providing encrypted and strongly authenticated remote login sessions.

SSH provides sessions between a host running a SSH server and a machine with a SSH client. The AlliedWare Plus™ OS includes both a SSH server and a SSH client to enable you to securely—with the benefit of cryptographic authentication and encryption—manage your devices over an insecure network:

- SSH replaces Telnet for remote terminal sessions; SSH is strongly authenticated and encrypted.
- Remote command execution allows you to send commands to a device securely and conveniently, without requiring a terminal session on the device.
- SSH allows you to connect to another host from your switch or router.

The AlliedWare Plus™ OS supports Secure Copy (SCP) and SSH File Transfer Protocol (SFTP). Both these protocols allow you to securely copy files between your device and remote machines. SFTP provides additional features from SCP, such as allowing you to manipulate the remote files, and halt or resume file transfers without closing the session.

Secure Shell on the AlliedWare Plus OS

The AlliedWare Plus™ OS implementation of SSH is compatible with the following RFCs and Internet Drafts:

- The Secure Shell (SSH) Protocol Architecture (RFC 4251)
- The Secure Shell (SSH) Authentication Protocol (RFC 4252)
- The Secure Shell (SSH) Transport Layer Protocol (RFC 4253)
- The Secure Shell (SSH) Connection Protocol (RFC 4254)
- The SSH (Secure Shell) Remote Login Protocol (draft-ylonen-ssh-protocol-00.txt)
- SSH File Transfer Protocol (draft-ietf-secsh-filexfer-13.txt)

Secure Shell supports the following features for both SSH version 2 and SSH version 1.5:

- Inbound SSH connections (server mode) and outbound SSH connections (client mode).
- File loading to and from remote machines using Secure Copy, using either the SSH client or SSH server mode.
- RSA public keys with lengths of 768–32768 bits, and DSA keys with lengths of 1024 bits. Keys are stored in a format compatible with other SSH implementations, and mechanisms are provided to copy keys to and from your device.
- Secure encryption, such as Triple DES and Blowfish.
- Remote non-interactive shell that allows arbitrary commands to be sent securely to your device, possibly automatically.
- Compression of Secure Shell traffic.
- Tunneling of TCP/IP traffic.

Secure Shell supports the following features for SSH version 2 only:

- File loading from remote machines using SSH File Transfer Protocol (SFTP).
- A login banner on the SSH server, that displays when SSHv2 clients connect to the server.

Configuring the SSH Server

This section provides instructions on:

- **Creating a Host Key**
- **Enabling the Server**
- **Modifying the Server**
- **Validating the Server Configuration**
- **Adding SSH Users**
- **Authenticating SSH Users**
- **Adding a Login Banner**
- **Monitoring the Server and Managing Sessions**
- **Debugging the Server**

Creating a Host Key

The SSH server uses either an RSA or DSA host key to authenticate itself with SSH clients. This key must be configured before the SSH server can operate. If no host key exists, you cannot start the SSH server.

Once created, the host key is stored securely on the device. To generate a host key for the SSH server, use the command:

```
awplus(config)# crypto key generate hostkey {dsa|rsa|rsa1}
                [<768-32768>]
```

This command has two parameters for creating RSA keys. The **rsa** parameter creates a host key for SSH version 2 sessions only. To create a host key for SSH version 1 sessions, use the **rsa1** parameter.

To destroy a host key, use the command:

```
awplus(config)# crypto key destroy hostkey {dsa|rsa|rsa1}
```

To display a host key stored on your device, use the command:

```
awplus(config)# show crypto key hostkey [dsa|rsa|rsa1]
```

Enabling the Server

You must enable the SSH server before connections from SSH, SCP, and SFTP clients are accepted. When the SSH server is disabled it rejects connections from SSH clients. The SSH server is disabled by default on your device.

To enable the SSH server, use the command:

```
awplus(config)# service ssh [ip|ipv6]
```

To disable the SSH server, use the command:

```
awplus(config)# no service ssh [ip|ipv6]
```

When enabled, the SSH server allows SCP and SFTP sessions by default. To disable these services, use the commands:

```
awplus(config)# no ssh server scp

awplus(config)# no ssh server sftp
```

This allows you to reject SCP or SFTP file transfer requests, while still allowing Secure Shell connections. To re-enable SCP and SFTP services, use the command:

```
awplus(config)# ssh server scp

awplus(config)# ssh server sftp
```

Modifying the Server

To modify the SSH version that the server supports, or the TCP port that the server listens to for incoming sessions, use the command:

```
awplus(config)# ssh server {[v1v2|v2only]|<1-65535>}
```

The server listens on port 22 for incoming sessions, and supports both SSH version 2 and SSH version 1, by default.

To modify session and login timeouts on the SSH server, and the number of unauthenticated connections the server allows, use the command:

```
awplus(config)# ssh server {[session-timeout <0-3600>]
               [login-timeout <1-600>]
               [max-startups <1-128>]}
```

The SSH server waits 60 seconds for a client to authenticate itself, by default. You can alter this waiting time by using the **login-timeout** parameter. If the client is still not authenticated after the set timeout, then the SSH server disconnects the session.

The SSH server only allows only 10 unauthenticated SSH sessions at any point in time, by default. You can modify the number of unauthenticated sessions it allows, by using the **max-startups** parameter.

Once a client has authenticated, the SSH session does not time out, by default. Use the **session-timeout** parameter to set a **maximum time period the server waits before deciding that a session is inactive and terminating it**

For example, to set the session timeout to 600 seconds, the login timeout to 30 seconds, and the maximum number of concurrent unauthenticated sessions to 5, use the command:

```
awplus(config)# ssh server session-timeout 600 login-timeout
               30 max-startups 5
```

To remove the configured session timeout, login timeout, or maximum startups, use the command:

```
awplus(config)# no ssh server session-timeout login-timeout
               max-startups
```

Validating the Server Configuration

To validate the SSH server configuration, use the command:

```
awplus(config)# show running-config ssh
```

Adding SSH Users

The SSH server requires you to register SSH users. Users that are not registered cannot access the SSH server. Ensure first that you have defined the user in the Authorized User Database of your device. To add a new user, use the command:

```
awplus(config)# username USERNAME (privilege 1-15) password
                PASSWORD
```

To register a user with the SSH server, use the command:

```
awplus(config)# ssh server allow-users <username-pattern>
                [<hostname-pattern>]
```

Registered entries can contain just the username, or the username with some host details, such as an IP address range. Additionally you can specify a range of users or hostname details by using an asterisk to match any string of characters. For example, to allow any user from the IP range 192.168.1.1 to 192.168.1.255, use the command:

```
awplus(config)# ssh server allow-users * 192.168.1.*
```

To display the list of allowed users, use the command:

```
awplus# show ssh server allow-users
```

To delete an entry from the list of allowed users, use the command:

```
awplus(config)# no ssh server allow-users <username-pattern>
                [<hostname-pattern>]
```

The SSH server also contains a list of denied users. The server checks all incoming sessions against this list and denies any matching session, regardless of whether the session matches an entry in the allowed users list. To add an entry to the list of denied users, use the command:

```
awplus(config)# ssh server deny-users <username-pattern>
                [<hostname-pattern>]
```

This allows you to deny specific users from a range of allowed users. For example, to deny a user with the IP address 192.168.1.12, use the command:

```
awplus(config)# ssh server deny-users * 192.168.1.12
```

To display the database of denied users, use the command:

```
awplus# show ssh server deny-users
```

To delete a client from the database of denied users, use the command:

```
awplus(config)# no ssh server deny-users <username-pattern>
                [<hostname-pattern>]
```

Authenticating SSH Users

SSH users can use either their password or public key authentication to authenticate themselves with the SSH server. To use public key authentication, copy the user's public key file from their client device to the SSH server. To associate the key with a user, use the command:

```
awplus(config)# crypto key pubkey-chain userkey <username>
                [<filename>]
```

For example, to associate the file key.pub with the user "langley", use the command:

```
awplus(config)# crypto key pubkey-chain userkey langley
                key.pub
```

To add a key as text into the terminal for user "geoff", first enter the command:

```
awplus(config)# crypto key pubkey-chain userkey geoff
```

then paste or type the key in as text.

You can add multiple keys for the same user. To display the list of public keys associated with a user, use the command:

```
awplus(config)# show crypto key pubkey-chain userkey
                <username> [<1-65535>]
```

The **<1-65535>** parameter allows you to display an individual key.

To delete a key associated with a user from your device, use the command:

```
awplus(config)# no crypto key pubkey-chain userkey
                <username> <1-65535>
```

Adding a Login Banner

You can add a login banner to the SSH server for sessions with SSH version 2 clients. The server displays the banner to clients before the login prompt. To set the login banner's message, use the command:

```
awplus(config)# banner login
```

then enter your message and use Ctrl+D to finish.

To view the configured login banner, use the command:

```
awplus# show banner login
```

To remove the configured message for the login banner, use the command:

```
awplus(config)# no banner login
```

Monitoring the Server and Managing Sessions

To display the current status of the SSH server, use the command:

```
awplus# show ssh server
```

To display the current status of SSH sessions on your device, use the command:

```
awplus# show ssh
```

Note that this displays both SSH server and SSH client sessions that your Allied Telesis device is running. Use this command to view the unique identification number assigned to each incoming or outgoing SSH session. You need the ID number when terminating a specific session from your device.

To terminate a session, or all sessions, use the command:

```
awplus# clear ssh {<1-65535>|all}
```

Debugging the Server

Information which may be useful for troubleshooting the SSH server is available using the SSH debugging function. You can enable server debugging while the SSH server is functioning. Use the command:

```
awplus# debug ssh server [brief|full]
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

Configuring the SSH Client

This section provides instructions on:

- **Modifying the Client**
- **Adding SSH Servers**
- **Authenticating with a Server**
- **Connecting to a Server and Running Commands**
- **Copying files to and from the Server**
- **Debugging the Client**

Modifying the Client

You can configure a selection of variables when using the SSH client. Note that the following configuration commands apply only to client sessions initiated after the command. The configured settings are not saved; after you have logged out from the SSH client, the client returns to using the default settings. Use the command:

```
awplus(config)# ssh client {port <1-65535>|version {1|2}|
                session-timeout <0-3600>|connect-timeout
                <1-600>}
```

The SSH client uses TCP port 22, by default. You can change the TCP port for the remote SSH server by using the **port** parameter.

The client supports both SSH version 1 and version 2 sessions, by default. To change the SSH client to only use a specific SSH version for sessions, for example SSH version 1, use the **version** parameter.

The client terminates sessions that are not established after 30 seconds, by default. You can change this time period by using the session-timeout parameter.

Once the client has authenticated with a server, the client does not time out the SSH session, by default. Use the **session-timeout** parameter to set a maximum time period the client waits before deciding that a session is inactive and terminating the session.

To modify the SSH client so that it uses port 2000 for sessions, and supports only SSH version 1 connections, use the command:

```
awplus(config# ssh client port 2000 version 1
```

To modify the SSH client so that unestablished sessions time out after 60 seconds, and inactive sessions time out after 100 seconds, use the command:

```
awplus(config)# ssh client session-timeout 100 connect-timeout
                100
```

To remove the configured port, SSH version, session timeout, and connection timeout settings, use the command:

```
awplus(config)# no ssh client port version session-timeout
                connect-timeout
```

Adding SSH Servers

SSH servers identify themselves using a host key (see **"Creating a Host Key" on page 52.4**). Before the SSH client establishes a session with a SSH server, it confirms that the host key sent by the server matches its database entry for the server. If the database does not contains a host key for the server, then the SSH client requires you to confirm that the host key sent from the server is correct.

To add an SSH server to the client's database, use the command:

```
awplus# crypto key pubkey-chain knownhosts [ip|ipv6]
       <hostname> [rsa|dsa|rsa1]
```

To display the SSH servers in the client's database, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
       [<1-65535>]
```

To remove an entry in the database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts <1-65535>
```

Authenticating with a Server

You can authenticate your session with a server by either using a password, or using RSA or DSA public key authentication. To use public key authentication, you must generate a pair of keys, one private and one public, and copy the public key onto the SSH server.

To generate an RSA or DSA set of private and public keys for an SSH user, use the command:

```
awplus(config)# crypto key generate userkey <username> {dsa|
                rsa|rsa1} [<768-32768>]
```

You can generate one key of each encryption type per user on your client. When authenticating with an SSH server that supports SSH version 1 only, you must use a key generated by the **rsa1** parameter.

To copy the public key onto the SSH server, you must display the key onscreen. To display the public key associated with a user, use the command:

```
awplus# show crypto key userkey <username> [dsa|rsa|
       rsa1]
```

To display the public keys set for other users, you must specify their username. Only users with the highest privilege setting can use this command to view the keys of other users.

To delete a public and private pair of keys associated with a user, use the command:

```
awplus(config)# crypto key destroy userkey <username> {dsa|rsa|
                rsa1}
```

Connecting to a Server and Running Commands

To connect to a remote SSH server and execute a command, use the command:

```
awplus# ssh [ip|ipv6][{[user <username>]|[port
        <1-65535>]|[version {1|2}]}] <hostname>
        [<line>]
```

By default, the SSH client attempts to use SSH version 2 with the SSH server. If this fails, the client uses SSH version 1.

For example, to connect to the SSH server at 192.168.1.2 as user “john”, and execute the command “show sys”, use the command:

```
awplus# ssh user john 192.168.1.2 “show sys”
```

Copying files to and from the Server

You can use either the SCP or SFTP client to transfer files from a remote SSH server. Use the command:

```
awplus# copy <source-url> <destination-url>
```

For example, to use SFTP to load a file from the SSH server 192.168.1.2, onto the flash memory of your device, use the command:

```
awplus# copy sftp://192.168.1.2/key.pub flash
```

To upload files to the SSH server, you must use SCP. For example, to upload the file bobskey.pub as the user “bob”, use the command:

```
awplus# copy flash:/bobskey.pub scp://bob@192.168.1.2
```

For more information see **Chapter 6, Creating and Managing Files**.

Debugging the Client

Information which may be useful for troubleshooting the SSH client is available using the SSH debugging function. You can enable client debugging while the SSH client is functioning. Use the command:

```
awplus# debug ssh client [brief|full]
```

To disable SSH client debugging, use the command:

```
awplus# no debug ssh client
```

Chapter 53: Secure Shell (SSH) Configuration

SSH Server Configuration Example 53.2

SSH Server Configuration Example

This chapter provides a Secure Shell server configuration example. For more information about the SSH server, see **Chapter 52, Secure Shell (SSH) Introduction**. For detailed information about the commands used to configure the SSH server, see **Chapter 54, Secure Shell (SSH) Commands**.

The following example configures a SSH server where:

- the SSH server uses RSA encryption
- the SSH server is compatible with both SSH version 1 and version 2 clients
- three SSH users are configured: Manager, John, and Asuka. “manager” can connect from only a defined range of hosts, while “john” and “asuka” can SSH from all hosts
- the SSH users use RSA private and public key authentication

This example shows how to create RSA encryption keys, configure the Secure Shell server, and register users to make Secure Shell connections to your device.

Step 1: Login as a highest Privileged User.

To create the keys and add users, you must login as a privileged user.

Step 2: Create encryption keys.

Two RSA private keys are required before enabling the Secure Shell server for each type of SSH version. Use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa
awplus(config)# crypto key generate hostkey rsa1
awplus(config)# exit
```

To verify the key creation, use the command:

```
awplus# show crypto key hostkey
```

Step 3: Enable the Secure Shell server.

Enable Secure Shell on the device using the commands:

```
awplus# configure terminal
awplus(config)# service ssh
```

Modify the SSH server settings as desired. For example, to set the login-timeout to 60, and the session-timeout to 3600, use the commands:

```
awplus(config)# ssh server session-timeout 3600 login-timeout
60
```

To verify the server configuration, use the command:

```
awplus# show ssh
```

Step 4: Create SSH users.

In order to connect and execute commands, you must register users in the SSH user database, and in the User Authentication Database of the device.

To create the users `john` and `asuka` in the User Authentication Database, use the commands:

```
awplus# configure terminal
awplus(config)# username john privilege 15 password secret
awplus(config)# username asuka privilege 15 password
very secret
```

To register `john` and `asuka` as SSH clients, use the commands:

```
awplus(config)# ssh server allow-users john
awplus(config)# ssh server allow-users asuka
```

To register “manager” as an SSH client so that can only connect from the IP address 192.168.1.1, use the command:

```
awplus(config)# ssh server allow-users manager 192.168.1.1
```

Step 5: Set up authentication.

SSH users cannot connect unless the server can authenticate them. There are two ways to authenticate an SSH session: password authentication, and RSA or DSA private/public key authentication. When using password authentication, the user must supply their User Authentication Database password.

To use private/public key authentication, copy the public keys for each user onto the device. To copy the files onto flash from the key directory of an attached TFTP server, use the command:

```
awplus# copy tftp://key/john.pub flash:/john.pub
awplus# copy tftp://key/asuka.pub flash:/asuka.pub
```

To associate the key file with each user, use the command:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey john john.pub
awplus(config)# crypto key pubkey-chain userkey asuka
asuka.pub
awplus(config)# crypto key pubkey-chain userkey manager
manager.pub
```

Chapter 54: Secure Shell (SSH) Commands

Introduction 54.2
Command List 54.2
banner login (SSH) 54.2
clear ssh 54.3
crypto key destroy hostkey 54.4
crypto key destroy userkey 54.5
crypto key generate hostkey 54.6
crypto key generate userkey 54.7
crypto key pubkey-chain knownhosts 54.8
crypto key pubkey-chain userkey 54.10
debug ssh client 54.12
debug ssh server 54.13
service ssh 54.14
show banner login 54.16
show crypto key hostkey 54.17
show crypto key pubkey-chain knownhosts 54.18
show crypto key pubkey-chain userkey 54.19
show crypto key userkey 54.20
show running-config ssh 54.21
show ssh 54.22
show ssh client 54.23
show ssh server 54.24
show ssh server allow-users 54.25
show ssh server deny-users 54.26
ssh 54.27
ssh client 54.29
ssh server 54.31
ssh server allow-users 54.33
ssh server authentication 54.35
ssh server deny-users 54.37
ssh server resolve-host 54.38
ssh server scp 54.39
ssh server sftp 54.40
undebug ssh client 54.41
undebug ssh server 54.41

Introduction

This chapter provides an alphabetical reference for commands used to configure Secure Shell (SSH). For more information, see **Chapter 52, Secure Shell (SSH) Introduction**, and **Chapter 53, Secure Shell (SSH) Configuration**.

Command List

banner login (SSH)

This command configures a login banner on the SSH server. This displays a message on the remote terminal of the SSH client before the login prompt. SSH client version 1 does not support this banner.

To add a banner, first enter the command **banner login**, and hit [Enter]. Write your message. You can use any character and spaces. Use Ctrl+D at the end of your message to save the text and re-enter the normal command line mode.

The banner message is preserved if the device restarts.

The **no** variant of this command deletes the login banner from the device.

Syntax

```
banner login
no banner login
```

Default No banner is defined by default.

Mode Global Configuration

Examples To set a login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# banner login

Type CNTL/D to finish.
... banner message comes here ...
^D
awplus(config)#
```

and enter the message. Use Ctrl+D to finish.

To remove the login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# no banner login
```

Related Commands **show banner login**

clear ssh

This command deletes Secure Shell sessions currently active on the device. This includes both incoming and outgoing sessions. The deleted sessions are closed. You can only delete an SSH session if you are a system manager or the user who initiated the session. If **all** is specified then all active SSH sessions are deleted.

Syntax `clear ssh {<1-65535>|all}`

Parameters	Description
`<1-65535>`	Specify a session ID in the range 1 to 65535 to delete a specific session.
`all`	Delete all SSH sessions.

Mode Privileged Exec

Examples To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

Related Commands **service ssh**
ssh

crypto key destroy hostkey

This command deletes the existing public and private keys of the SSH server. Note that for an SSH server to operate it needs at least one set of hostkeys configured before an SSH server is started.

Syntax `crypto key destroy hostkey {dsa|rsa|rsa1}`

Parameters	Description
`dsa`	Deletes the existing DSA public and private keys.
`rsa`	Deletes the existing RSA public and private keys configured for SSH version 2 connections.
`rsa1`	Deletes the existing RSA public and private keys configured for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

Related Commands **crypto key generate hostkey**
service ssh

crypto key destroy userkey

This command destroys the existing public and private keys of an SSH user configured on the device.

Syntax `crypto key destroy userkey <username> {dsa|rsa|rsa1}`

Parameters	Description
`<username>`	Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
`dsa`	Deletes the existing DSA userkey.
`rsa`	Deletes the existing RSA userkey configured for SSH version 2 connections.
`rsa1`	Deletes the existing RSA userkey for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

Related Commands
crypto key generate hostkey
show ssh
show crypto key hostkey

crypto key generate hostkey

This command generates public and private keys for the SSH server using either an RSA or DSA cryptography algorithm. You must define a host key before enabling the SSH server. Start SSH server using the **service ssh** command. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax `crypto key generate hostkey {dsa|rsa|rsa1} [<768-32768>]`

Parameters	Description
`dsa`	Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey.
`rsa`	Creates an RSA hostkey for SSH version 2 connections.
`rsa1`	Creates an RSA hostkey for SSH version 1 connections.
<768-32768>	The length in bits of the generated key. The default is 1024 bits.

Default 1024 bits is the default key length. The DSA algorithm supports 1024 bits.

Mode Global Configuration

Examples To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

Related Commands
crypto key destroy hostkey
service ssh
show crypto key hostkey

crypto key generate userkey

This command generates public and private keys for an SSH user using either an RSA or DSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax `crypto key generate userkey <username> {dsa|rsa|rsa1} [<768-32768>]`

Parameters	Description
<username>	Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
`dsa`	Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.
`rsa`	Creates an RSA userkey for SSH version 2 connections.
`rsa1`	Creates an RSA userkey for SSH version 1 connections.
<768-32768>	The length in bits of the generated key. The DSA algorithm supports only 1024 bits. Default: 1024.

Mode Global Configuration

Examples To generate a 2048-bits RSA user key for SSH version 2 connections for the user `bob`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 2048
```

To generate a DSA user key for the user `lapo`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo dsa
```

Related Commands **crypto key destroy userkey**
show crypto key userkey

crypto key pubkey-chain knownhosts

This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

Syntax

```
crypto key pubkey-chain knownhosts [ip|ipv6] <hostname> [rsa|dsa|
   rsa1]

no crypto key pubkey-chain knownhosts <1-65535>
```

Parameter	Description
`ip`	Keyword used prior to specifying an IPv4 address
`ipv6`	Keyword used prior to specifying an IPv6 address
<hostname>	IPv4/IPv6 address or hostname of a remote server in the format `a.b.c.d` for an IPv4 address, or in the format `x:x::x:x` for an IPv6 address.
`rsa`	Specify the RSA public key of the server to be added to the known host database.
`dsa`	Specify the DSA public key of the server to be added to the known host database.
`rsa1`	Specify the SSHv1 public key of the server to be added to the know host database.
<1-65535>	Specify a key identifier when removing a key using the **no** parameter.

Default If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

Mode Privilege Exec

Usage This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

Examples

To add the RSA host key of the remote SSH host IPv4 address `192.0.2.11` to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

Validation Commands

show crypto key pubkey-chain knownhosts

crypto key pubkey-chain userkey

This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The **no** variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user's public key is removed, the SSH user can no longer login using public key authentication.

Syntax

```
crypto key pubkey-chain userkey <username> [<filename>]
no crypto key pubkey-chain userkey <username> <1-65535>
```

Parameters	Description
<username>	Name of the user that the SSH server associates the key with. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. Default: no default
<filename>	Filename of a key saved in flash. Valid characters are any printable character. You can add a key as a hexadecimal string directly into the terminal if you do not specify a filename.
<1-65535>	The key ID number of the user's key. Specify the key ID to delete a key.

Mode Global Configuration

Usage You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command **crypto key pubkey-chain userkey** <***username***>, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the **crypto key generate host rsa** command. View the SSH RSA key generated on the device using the **show crypto hostkey rsa** command. Copy and paste the displayed SSH RSA key after entering the **crypto key pubkey-chain userkey** <***username***> command. Use [Ctrl]+D after entering it to save it.

Examples To generate a valid SSH RSA key on the device and add the key, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto key generate host rsa
awplus(config)# exit
awplus# show crypto key hostkey rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J
20bWluhnUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9
IQe66+5YyD4UxOKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16
+6NvNbk+h+c/pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=

awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey joe
Type CNTL/D to finish:
AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J
20bWluhnUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9
IQe66+5YyD4UxOKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16
+6NvNbk+h+c/pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=
control-D
awplus(config)#
```

To add a public key for the user `graydon` from the file `key.pub`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey graydon key.pub
```

To add a public key for the user `tamara` from the terminal, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey tamara
```

and enter the key. Use Ctrl+D to finish.

To remove the first key entry from the public key chain of the user `john`, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain userkey john 1
```

Related Commands **show crypto key pubkey-chain userkey**

debug ssh client

This command enables the SSH client debugging facility. When enabled, any SSH, SCP and SFTP client sessions send diagnostic messages to the login terminal.

The **no** variant of this command disables the SSH client debugging facility. This stops the SSH client from generating diagnostic debugging message.

Syntax

```
debug ssh client [brief|full]
no debug ssh client
```

Parameter	Description
`brief`	Enables brief debug mode.
`full`	Enables full debug mode.

Default SSH client debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To start SSH client debugging, use the command:

```
awplus# debug ssh client
```

To start SSH client debugging with extended output, use the command:

```
awplus# debug ssh client full
```

To disable SSH client debugging, use the command:

```
awplus# no debug ssh client
```

Related Commands
debug ssh server
show ssh client
undebug ssh client

debug ssh server

This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

Syntax

```
debug ssh server [brief|full]
no debug ssh server
```

Parameter	Description
`brief`	Enables brief debug mode.
`full`	Enables full debug mode.

Default SSH server debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

Related Commands

debug ssh client
show ssh server
undebug ssh server

service ssh

This command enables the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

SSH server needs a host key before it starts. If an SSHv2 host key does not exist, then this command fails. If SSHv1 is enabled but a host key for SSHv1 does not exist, then SSH service is unavailable for version 1.

The **no** variant of this command disables the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the **clear ssh** command.

Syntax

```
service ssh [ip|ipv6]
no service ssh [ip|ipv6]
```

Default The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

Mode Global Configuration

Examples To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh
```

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ipv6
```

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh
```

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ipv6
```

Related Commands

crypto key generate hostkey
show running-config ssh
show ssh server
ssh server allow-users
ssh server deny-users

show banner login

This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

Syntax `show banner login`

Mode User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

Example To display the current login banner message, use the command:

```
awplus# show banner login
```

Related Commands banner login (SSH)

show crypto key hostkey

This command displays the SSH host keys generated by RSA and DSA algorithm.

A host key pair (public and private keys) is needed to enable SSH server. The private key remains on the device secretly. The public key is copied to SSH clients to identify the server

Syntax

```
show crypto key hostkey [dsa|rsa|rsa1]
```

Parameter	Description
dsa	Displays the DSA algorithm public key.
rsa	Displays the RSA algorithm public key for SSH version 2 connections.
rsa1	Displays the RSA algorithm public key for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

Output **Figure 54-1: Example output from the show crypto key hostkey command**

```
Type Bits   Fingerprint
-------------------------------------------------------------
rsa  2058   4e:7d:1d:00:75:79:c5:cb:c8:58:2e:f9:29:9c:1f:48
dsa  1024   fa:72:3d:78:35:14:cb:9a:1d:ca:1c:83:2c:7d:08:43
rsa1 1024   e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b
```

Table 54-1: Parameters in output of the show crypto key hostkey command

Parameter	Description
Type	Algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the public key.

Related Commands crypto key destroy hostkey
crypto key generate hostkey

show crypto key pubkey-chain knownhosts

This command displays the list of public keys maintained in the known host database on the device.

Syntax `show crypto key pubkey-chain knownhosts [<1-65535>]`

Parameter	Description
<1-65535>	Key identifier for a specific key. Displays the public key of the entry if specified.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Examples To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

Output **Figure 54-2: Example output from the show crypto key public-chain knownhosts command**

```
No     Hostname         Type Fingerprint
-------------------------------------------------------------------------
1      172.16.23.1      rsa  c8:33:b1:fe:6f:d3:8c:81:4e:f7:2a:aa:a5:be:df:18
2      172.16.23.10     rsa  c4:79:86:65:ee:a0:1d:a5:6a:e8:fd:1d:d3:4e:37:bd
3      5ffe:1053:ac21:ff00:0101:bcdf:ffff:0001
                        rsa1 af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57
```

Table 54-2: Parameters in the output of the show crypto key public-chain knownhosts command

Parameter	Description
`No`	Number ID of the key.
`Hostname`	Host name of the known SSH server.
`Type`	The algorithm used to generate the key.
`Fingerprint`	Checksum value for the public key.

Related Commands crypto key pubkey-chain knownhosts

show crypto key pubkey-chain userkey

This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

Syntax `show crypto key pubkey-chain userkey <username> [<1-65535>]`

Parameter	Description
<username>	User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
<1-65535>	Key identifier for a specific key.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the public keys for the user `manager` that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

Output **Figure 54-3: Example output from the show crypto key public-chain userkey command**

```
No Type Bits Fingerprint
--------------------------------------------------------------------
1  dsa  1024 2b:cc:df:a8:f8:2e:8f:a4:a5:4f:32:ea:67:29:78:fd
2  rsa  2048 6a:ba:22:84:c1:26:42:57:2c:d7:85:c8:06:32:49:0e
```

Table 54-3: Parameters in the output of the show crypto key userkey command

Parameter	Description
`No`	Number ID of the key.
`Type`	The algorithm used to generate the key.
`Bits`	Length in bits of the key.
`Fingerprint`	Checksum value for the key.

Related Commands crypto key pubkey-chain userkey

show crypto key userkey

This command displays the public keys created on this device for the specified SSH user.

Syntax `show crypto key userkey <username> [dsa|rsa|rsa1]`

Parameter	Description
<username>	User name of the local SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Displays the DSA public key.
rsa	Displays the RSA public key used for SSH version 2 connections.
rsa1	Displays the RSA key used for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public key generated for the user, use the command:

```
awplus# show crypto key userkey manager
```

To store the RSA public key generated for the user manager to the file "user.pub", use the command:

```
awplus# show crypto key userkey manager rsa > manager-rsa.pub
```

Output **Figure 54-4: Example output from the show crypto key userkey command**

```
Type Bits   Fingerprint
---------------------------------------------------------------
rsa  2048   e8:d6:1b:c0:f4:b6:e6:7d:02:2e:a9:d4:a1:ca:3b:11
rsa1 1024   12:25:60:95:64:08:8e:a1:8c:3c:45:1b:44:b9:33:9b
```

Table 54-4: Parameters in the output of the show crypto key userkey command

Parameter	Description
Type	The algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the key.

Related Commands crypto key generate userkey

show running-config ssh

This command displays the current running configuration of Secure Shell (SSH).

Syntax `show running-config ssh`

Mode Privileged Exec and Global Configuration

Example To display the current configuration of SSH, use the command:

```
awplus# show running-config ssh
```

Output **Figure 54-5: Example output from the show running-config ssh command**

```
!
ssh server session-timeout 600
ssh server login-timeout 30
ssh server allow-users manager 192.168.1.*
ssh server allow-users john
ssh server deny-user john*.a-company.com
ssh server
```

Table 54-5: Parameters in the output of the show running-config ssh command

Parameter	Description
`ssh server`	SSH server is enabled.
`ssh server v2`	SSH server is enabled and only support SSHv2.
`ssh server <port>`	SSH server is enabled and listening on the specified TCP port.
`no ssh server scp`	SCP service is disabled.
`no ssh server sftp`	SFTP service is disabled.
`ssh server session-timeout`	Configure the server session timeout.
`ssh server login-timeout`	Configure the server login timeout.
`ssh server max-startups`	Configure the maximum number of concurrent sessions waiting authentication.
`no ssh server authentication password`	Password authentication is disabled.
`no ssh server authentication publickey`	Public key authentication is disabled.
`ssh server allow-users`	Add the user (and hostname) to the allow list.
`ssh server deny-users`	Add the user (and hostname) to the deny list.

Related Commands **service ssh**
show ssh server

show ssh

This command displays the active SSH sessions on the device, both incoming and outgoing.

Syntax `show ssh`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current SSH sessions on the device, use the command:

```
awplus# show ssh
```

Output **Figure 54-6: Example output from the show ssh command**

```
Secure Shell Sessions:
ID  Type Mode   Peer Host    Username   State       Filename
-------------------------------------------------------------------
414 ssh  server 172.16.23.1  root       open
456 ssh  client 172.16.23.10 manager    user-auth
459 scp  client 172.16.23.12 root       download    550dev_.awd
463 ssh  client 5ffe:33fe:5632:ffbb:bc35:ddee:0101:ac51
                             manager    user-auth
```

Table 54-6: Parameters in the output of the show ssh command

Parameter	Description	
ID	Unique identifier for each SSH session.	
Type	Session type; either SSH, SCP, or SFTP.	
Mode	Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session.	
Peer Host	The hostname or IP address of the remote server or client.	
Username	Login user name of the server.	
State	The current state of the SSH session. One of:	
	connecting	The device is looking for a remote server.
	connected	The device is connected to the remote server.
	accepted	The device has accepted a new session.
	host-auth	host-to-host authentication is in progress.
	user-auth	User authentication is in progress.
	authenticated	User authentication is complete.
	open	The session is in progress.
	download	The user is downloading a file from the device.
	upload	The user is uploading a file from the device.
	closing	The user is terminating the session.
	closed	The session is closed.
Filename	Local filename of the file that the user is downloading or uploading.	

Related Commands clear ssh

show ssh client

This command displays the current configuration of the Secure Shell client.

Syntax `show ssh client`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current configuration for SSH clients on the login shell, use the command:

```
awplus# show ssh client
```

Output **Figure 54-7: Example output from the show ssh client command**

```
Secure Shell Client Configuration
-----------------------------------------------------------------
Port                                : 22
Version                             : 2,1
Connect Timeout                     : 30 seconds
Session Timeout                     : 0 (off)
Debug                               : NONE
```

Table 54-7: Parameters in the output of the show ssh client command

Parameter	Description
`Port`	SSH server TCP port where the SSH client connects to. The default is port 22.
`Version`	SSH server version; either “1”, “2” or “2,1”.
`Connect Timeout`	Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout.
`Debug`	Whether debugging is active on the client.

Related Commands **show ssh server**

show ssh server

This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

Syntax `show ssh server`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

Output **Figure 54-8: Example output from the show ssh server command**

```
Secure Shell Server Configuration
-----------------------------------------------------------------
SSH Server                          : Enabled
Port                                : 22
Version                             : 2
Services                            : scp, sftp
User Authentication                 : publickey, password
Idle Timeout                        : 60 seconds
Maximum Startups                    : 10
Debug                               : NONE
```

Table 54-8: Parameters in the output of the show ssh server command

Parameter	Description
`SSH Server`	Whether the Secure Shell server is enabled or disabled.
`Port`	TCP port where the Secure Shell server listens for connections. The default is port 22.
`Version`	SSH server version; either “1”, “2” or “2,1”.
`Services`	List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.
`Authentication`	List of available authentication methods.
`Login Timeout`	Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches.
`Idle Timeout`	Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off.
`Maximum Startups`	The maximum number of concurrent connections that are waiting authentication. The default is 10.
`Debug`	Whether debugging is active on the server.

Related Commands **show ssh**
show ssh client

show ssh server allow-users

This command displays the user entries in the allow list of the SSH server.

Syntax `show ssh server allow-users`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the allow list of the SSH server, use the command:

```
awplus# show ssh server allow-users
```

Output **Figure 54-9: Example output from the show ssh server allow-users command**

```
Username          Remote Hostname (pattern)
----------------- ------------------------------
awplus            192.168.*
john
manager           *.alliedtelesis.com
```

Table 54-9: Parameters in the output of the show ssh server allow-users command

Parameter	Description
`Username`	User name that is allowed to access the SSH server.
`Remote Hostname (pattern)`	IP address or hostname pattern of the remote client. The user is allowed requests from a host that matches this pattern. If no hostname is specified, the user is allowed from all hosts.

Related Commands **ssh server allow-users**
ssh server deny-users

show ssh server deny-users

This command displays the user entries in the deny list of the SSH server. The user in the deny list is rejected to access the SSH server. If a user is not included in the access list of the SSH server, the user is also rejected.

Syntax `show ssh server deny-users`

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the deny list of the SSH server, use the command:

```
awplus# show ssh server deny-users
```

Output **Figure 54-10: Example output from the show ssh server deny-user command**

```
Username          Remote Hostname (pattern)
----------------- --------------------------------
john              *.b-company.com
manager           192.168.2.*
```

Table 54-10: Parameters in the output of the show ssh server deny-user command

Parameter	Description
`Username`	The user that this rule applies to.
`Remote Hostname (pattern)`	IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts.

Related Commands ssh server allow-users
ssh server deny-users

ssh

This command initiates a Secure Shell connection to a remote SSH server.

If the server requests a password for the user login, the user needs to type in the correct password on “Password:” prompt.

SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

Note Note that any hostname specified with ssh cannot begin with a hyphen (-) character.

Syntax

```
ssh [ip|ipv6][{[user <username>]|[port <1-65535>]|[version {1|2}]}]
   <hostname> [<line>]
```

Parameter	Description	
`ip`	Specify IPv4 SSH.	
`ipv6`	Specify IPv6 SSH.	
`user`	Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.	
	<username>	User name to login on the remote server.
`port`	SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Other- wise, the client port configured by “ssh client” command or the default TCP port (22) is used.	
	<1-65535>	TCP port.
`version`	SSH client version. If version is specified, the SSH client supports only the specified SSH version. By default, SSH client uses SSHv2 first. If the server does not support SSHv2, it will try SSHv1. The default version can be configured by “ssh client” command.	
	`1`	Use SSH version 1.
	`2`	Use SSH version 2.
<hostname>	IPv4/IPv6 address or hostname of a remote server in the format `a.b.c.d` for an IPv4 address, or in the format `x:x::x:x` for an IPv6 address corresponding to the ip or ipv6 optional keywords used. Note that any hostname specified with ssh cannot begin with a hyphen (-) character.	
	<line>	Command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.

Mode User Exec and Privileged Exec

Examples To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user **manager**, use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server with example_host using IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

Related Commands
crypto key generate userkey
crypto key pubkey-chain knownhosts
debug ssh client
ssh client

ssh client

This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the **ssh client** command, and restores the defaults.

This command does not affect the existing SSH sessions.

Syntax

```
ssh client {port <1-65535>|version {1|2}|session-timeout <0-3600>|
    connect-timeout <1-600>}

no ssh client {port|version|session-timeout|connect-timeout}
```

Parameter	Description	
`port`	The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port. Default: **22**	
	<1-65535>	TCP port number.
`version`	The SSH version used by the client for SSH sessions. The SSH client supports both version 2 and version 1 Default: **version 2** **Note**: SSH version 2 is the default SSH version. SSH client supports SSH version 1 if SSH version 2 is not configured using a **ssh version** command.	
	`1`	SSH clients on the device supports SSH version 1 only.
	`2`	SSH clients on the device supports SSH version 2 only
`session-timeout`	The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout. Default: **0** (session timer remains off)	
	<0-3600>	Timeout in seconds.
`connect-timeout`	The maximum time period that an SSH session can take to become established. The SSH client terminates the SSH session if this timeout expires and the session is still not established. Default: **30**	
	<1-600>	Timeout in seconds.

Mode Privileged Exec

Examples

To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

Related Commands

show ssh client
ssh

ssh server

This command modifies the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

The **no** variant of this command restores the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the **service ssh** command.

Syntax

```
ssh server {[v1v2|v2only]|<1-65535>}
ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]
    [max-startups <1-128>]}
no ssh server {[session-timeout] [login-timeout] [max-startups]}
```

Parameter	Description
`v1v2`	Supports both SSHv2 and SSHv1client connections. Default: **v1v2**
`v2only`	Supports SSHv2 client connections only.
<1-65535>	The TCP port number that the server listens to for incoming SSH sessions. Default: **22**
`session-timeout`	There is a maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages. Default: **0** (session timer remains off).
<0-3600>	Timeout in seconds.
`login-timeout`	The maximum time period the server waits before disconnecting an unauthenticated client. Default: **60**
<1-600>	Timeout in seconds.
`max-startups`	The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection. Default: **10**
<1-128>	Number of sessions.

Mode Global Configuration

Examples

To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting authentication from SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v1v2
```

Related Commands

show ssh server
ssh client

ssh server allow-users

This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server allow-users <username-pattern> [<hostname-pattern>]
no ssh server allow-users <username-pattern> [<hostname-pattern>]
```

Parameter	Description
<username-pattern>	The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.
<*hostname-pattern*>	The host name pattern that hosts can match to. If specified, the server allows the user to connect only from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.

Mode Global Configuration

Examples To allow the user `john` to create an SSH session from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john
```

To allow the user `john` to create an SSH session from a range of IP address (from 192.168.1.1 to 192.168.1.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john 192.168.1.*
```

To allow the user `john` to create a SSH session from `a-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john *.a-company.com
```

To delete the existing user entry `john 192.168.1.*` in the allow list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server allow-users john 192.168.1.*
```

Related Commands

show running-config ssh
show ssh server allow-users
ssh server deny-users

ssh server authentication

This command enables RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **ssh server authentication** command to enable password authentication for users. Apply the **publickey** keyword with the **ssh server authentication** command to enable RSA public-key authentication for users.

Use the **no** variant of this command to disable RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **no ssh authentication** command to disable password authentication for users. Apply the required **publickey** keyword with the **no ssh authentication** command to disable RSA public-key authentication for users.

Syntax

```
ssh server authentication {password|publickey}
no ssh server authentication {password|publickey}
```

Parameter	Description
`password`	Specifies user password authentication for SSH server.
`publickey`	Specifies user publickey authentication for SSH server.

Default Both RSA public-key authentication and password authentication are enabled by default.

Mode Global Configuration

Usage For password authentication to authenticate a user, password authentication for a user must be registered in the local user database or on an external RADIUS server, before using the **ssh server authentication password** command.

For RSA public-key authentication to authenticate a user, a public key must be added for the user, before using the **ssh server authentication publickey** command.

Examples To enable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication password
```

To enable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication publickey
```

To disable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication password
```

To disable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication publickey
```

Related Commands

crypto key pubkey-chain userkey
service ssh
show ssh server

ssh server deny-users

This command adds a username pattern to the deny list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is rejected.

SSH server also maintains the allow list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

If a hostname pattern is specified, the user is denied from the hosts matching the pattern.

The **no** variant of this command deletes a username pattern from the deny list of the SSH server. To delete an entry from the deny list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server deny-users <username-pattern> [<hostname-pattern>]
no ssh server deny-users <username-pattern> [<hostname-pattern>]
```

Parameter	Description
<username-pattern>	The username pattern that users can match to. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen, full stop and asterisk symbols. An asterisk acts as a wildcard character that matches any string of characters.
<hostname-pattern>	The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.

Mode Global Configuration

Examples To deny the user `john` to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user john to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user `john` to access SSH login from `b-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```

To delete the existing user entry `john 192.168.2.*` in the deny list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server deny-users john 192.168.2.*
```

Related Commands
show running-config ssh
show ssh server deny-users
ssh server allow-users

ssh server resolve-host

This command enables resolving an IP address from a host name using a DNS server for client host authentication.

The **no** variant of this command disables this feature.

Syntax

```
ssh server resolve-hosts
no ssh server resolve-hosts
```

Default This feature is disabled by default.

Mode Global Configuration

Usage Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. To add a DNS server to the list of servers that the device sends DNS queries to use the **ip name-server** command on page 25.17.

For information about configuring DNS see **"DNS Client" on page 24.6**.

Example To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

Related Commands
ip name-server
show ssh server
ssh server allow-users
ssh server deny-users

ssh server scp

This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

Syntax

```
ssh server scp
no ssh server scp
```

Mode Global Configuration

Examples To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

Related Commands

show running-config ssh
show ssh server

ssh server sftp

This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

Syntax

```
ssh server sftp
no ssh server sftp
```

Mode Global Configuration

Examples To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

Related Commands **show running-config ssh**
show ssh server

undebug ssh client

This command applies the functionality of the **no debug ssh client** command.

undebug ssh server

This command applies the functionality of the **no debug ssh server** command.

Chapter 55: DHCP Snooping Introduction and Configuration

Introduction 55.2
DHCP Snooping 55.2
- DHCP Snooping Database 55.3
- DHCP Relay Agent Option 82 ..... 55.4
- Traffic Filtering with DHCP Snooping 55.6
- ARP Security 55.8
- MAC Address Verification 55.8
- DHCP Snooping Violations 55.8

Interactions with Other Features 55.9
Configuration 55.10
- Configure DHCP Snooping 55.10
- Disabling DHCP Snooping 55.16
- Related Features 55.16

Introduction

This chapter provides information about DHCP snooping, support for it on this switch, and how to configure it.

For detailed descriptions of the commands used to configure DHCP snooping, see **Chapter 56, DHCP Snooping Commands**; for related ACL commands, see **Chapter 37, IPv4 Hardware Access Control List (ACL) Commands**.

For information about Dynamic Host Configuration protocol and how to configure it, see **Chapter 64, Dynamic Host Configuration Protocol (DHCP) Introduction** and **Chapter 65, Dynamic Host Configuration Protocol (DHCP) Commands**.

DHCP Snooping

DHCP snooping provides an extra layer of security on the switch via dynamic IP source filtering. DHCP snooping filters out traffic received from unknown, or 'untrusted' ports, and builds and maintains a DHCP snooping database.

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP addresses to client devices. The use of dynamically assigned addresses requires traceability, so that a service provider can determine which clients own a particular IP address at a certain time.

With DHCP snooping, IP sources are dynamically verified, and filtered accordingly. IP packets that are not sourced from recognized IP addresses can be filtered out. This ensures the required traceability.

With DHCP snooping, an administrator can control port-to-IP connectivity by:

- permitting port access to specified IP addresses only
- permitting port access to DHCP issued IP addresses only
- dictating the number of IP clients on any given port
- passing location information about an IP client to the DHCP server
- permitting only known IP clients to ARP

Ports on the switch are classified as either trusted or untrusted:

- Trusted ports receive only messages from within your network.
- Untrusted ports receive messages from outside your network.

DHCP snooping blocks unauthorized IP traffic from untrusted ports, and prevents it from entering the trusted network. It validates DHCP client packets from untrusted ports and forwards them to trusted ports in the VLAN.

On this switch, DHCP snooping is disabled by default, and can be enabled on per-VLAN basis to operate over switch ports and over static and dynamic (LACP) link aggregators (channel groups).

DHCP Snooping Database

When you enable DHCP snooping, the switch intercepts all DHCP packets it receives, and sends them to the Central Processing Unit (CPU), where they are verified. The DHCP snooping database stores and maintains this information. The database contains entries for:

- current IP address leases dynamically allocated by a DHCP server
- static or dynamic entries added from the command line—typically used to add a DHCP snooping entry for a client that has a preconfigured IP address on an untrusted port

Database backup

The switch periodically saves the dynamic entries in the DHCP snooping database to a hidden file (**.dhcp.dsn.gz**) in Non-Volatile Storage (NVS), or can be configured to save them to Flash memory or to a USB memory device.

If such a database file exists, it is loaded when the switch starts up with DHCP snooping enabled, or when DHCP snooping is subsequently enabled.

Lease entries

Each entry in the database corresponds to a DHCP IP address lease.

For dynamic entries added automatically by DHCP snooping, each entry contains the following information:

- the IP address that was allocated to that client
- the MAC address of the client device
- the time until expiry
- the VLAN to which the client is attached
- the port to which the client is attached
- the IP address of the DHCP server

For static entries added from the command line, each entry contains the following subset of information:

- the IP address allocated to the client
- the MAC address of the client device (optional)
- the VLAN to which the client is attached
- the port to which the client is attached

Each entry also shows its source: Dynamic or Static.

On this switch, the maximum number of lease entries that can be stored in the DHCP snooping database for each port can be configured—the default is 1.

Expired entries

For dynamic entries, the switch receives expiry information with the client lease information in DHCP packets. Entries expire when the time left to expiry is 0 seconds. Expired entries are automatically deleted from the database. Static entries have no expiry information, and are not checked. All dynamic entries in the database are written to the backup file. Whenever DHCP snooping is enabled, the DHCP snooping database is repopulated from the backup file and any static entries in the start-up configuration file. Any entries present in the backup file that have expired are ignored.

DHCP Relay Agent Option 82

If the switch is at the edge of the network, it can be configured to insert DHCP Relay Agent Option 82 information into client-originated BOOTP/DHCP packets that it is forwarding to a DHCP server. The switch also removes DHCP Relay Agent Option 82 information from BOOTP reply packets destined for an untrusted port if the DHCP client hardware is directly attached to a port on the switch.

DHCP servers that are configured to recognize DHCP Relay Agent Option 82 may use the information to implement IP address or other parameter assignment policies, based on the network location of the client device.

When DHCP Relay Agent Option 82 information for DHCP snooping is enabled, the switch inserts DHCP Relay Agent Option 82 information into BOOTP request packets received from an untrusted port. The switch inserts the following DHCP Relay Agent Option 82 information:

- Remote ID: this identifies the host. By default, this is the MAC address of the switch (sub-option1).
- Circuit ID: this specifies the switch port and VLAN ID that the client-originated DHCP packet was received on (sub-option2). By default, this is the VLAN ID and the Ifindex (interface number).
- Subscriber ID (optional): this is a string of up to 50 characters that differentiates or groups client ports on the switch (sub-option 6).

Support on this switch

This switch inserts DHCP Relay Agent Option 82 (agent option) information into DHCP packets received through untrusted ports, and removes it from DHCP packets transmitted through untrusted ports. This is enabled by default, and can be disabled if required.

You can specify values for the Remote ID and Circuit ID sub-options of the DHCP Relay Agent Option 82 field. The Remote ID can be specified as an alphanumeric (ASCII) string, 1 to 63 characters in length. The Circuit ID can be specified as the VLAN ID and port number.

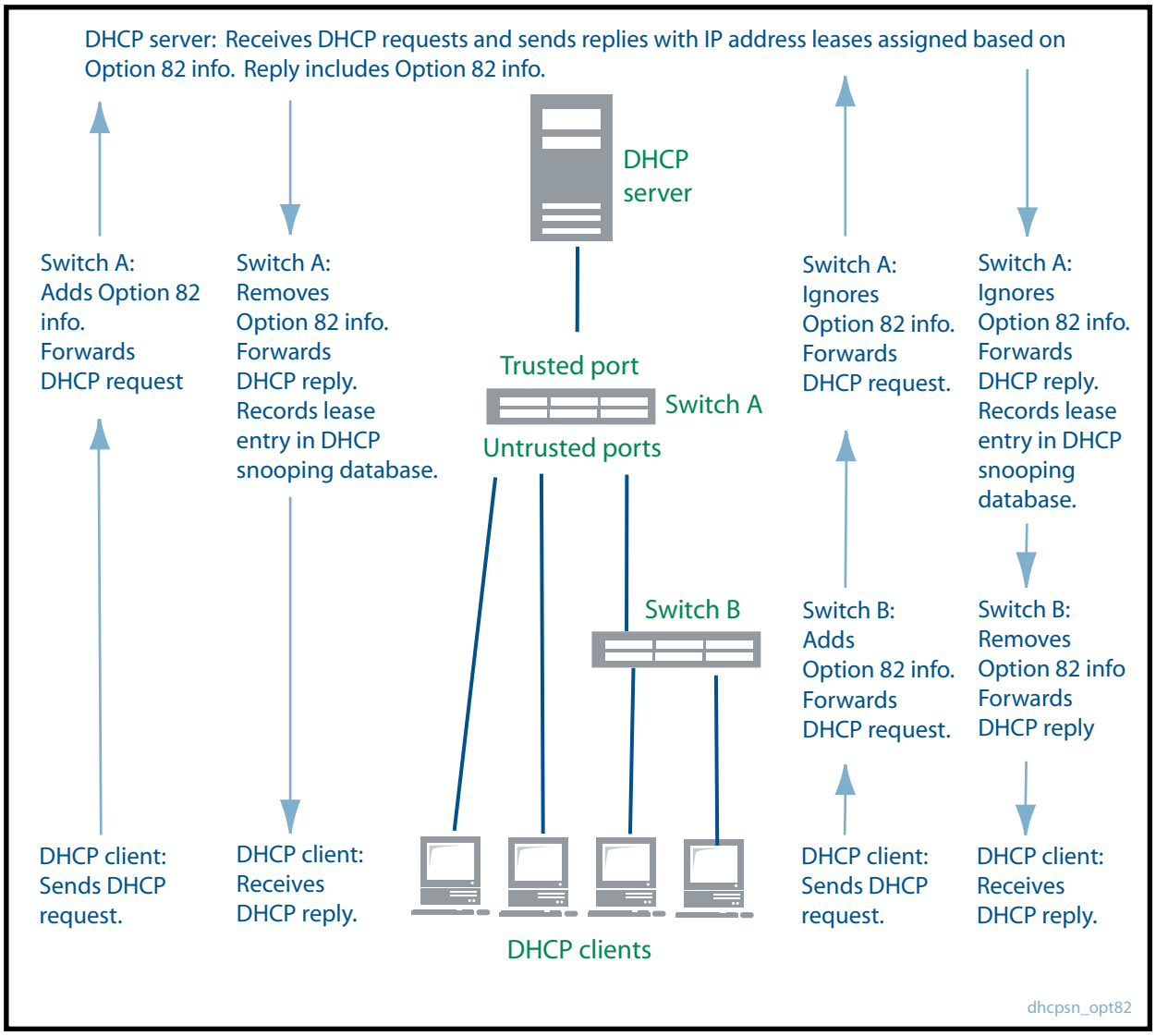
Subscriber IDs can be configured for ports, and if they have been configured, they are inserted in DHCP packets as part of the DHCP Relay Agent Option 82 information.

Regardless of whether DHCP Relay Agent Option 82 is enabled for DHCP snooping, if the switch receives a BOOTP/DHCP request packet on a trusted port, and the packet contains DHCP Relay Agent Option 82 information, it does not update the DHCP Relay Agent Option 82 information for the receiver port. By default, if it receives a DHCP request packet containing DHCP Relay Agent Option 82 information on an untrusted port, it drops the packet. However, if the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports—the switch can be configured to forward these packets.

Operation **Figure 55-1** shows DHCP packet flow between DHCP clients and server, where:

- Switch A has DHCP snooping enabled. The DHCP server is connected to a trusted port on Switch A; DHCP clients and Switch B are connected to untrusted ports.
- Switch A is configured to add and remove DHCP Relay Agent Option 82 information (**ip dhcp snooping agent-option** command on page 56.10).
- Switch A is configured to forward DHCP packets that already contain DHCP Relay Agent Option 82 information without changing it (**ip dhcp snooping agent-option allow-untrusted** command on page 56.11).
- Switch B is Layer 2 switching traffic from downstream DHCP clients, and adds and removes DHCP Relay Agent Option 82 information.

Figure 55-1: DHCP packet flow with DHCP snooping and DHCP Relay Agent Option 82 (agent option)



For more information about DHCP Relay Agent Option 82, see RFC 3046, DHCP Relay Agent Information Option.

Traffic Filtering with DHCP Snooping

DHCP filtering prevents IP addresses from being falsified or 'spoofed'. This guarantees that users cannot avoid detection by spoofing IP addresses that are not actually allocated to them. With DHCP filtering, the switch permits packets to enter over a specific port if their source IP address is currently allocated to a client connected to that port.

Support on this switch

On this switch, Access Control Lists (ACLs) based on DHCP snooping can be used with access groups to filter IP packets. For instance, IP traffic on untrusted ports can be limited to packets matching valid DHCP lease information stored in the DHCP snooping database. Quality of Service (QoS) configuration can also be applied to these ACLs.

The DHCP snooping feature is enabled or disabled per VLAN, and several of the related configuration settings are applied per port. If there are multiple VLANs on a port, all the VLANs will be subject to the same per-port settings.

Operation

Table 55-1 on page 55.7 shows the filtering that is applied by DHCP snooping on a switch with the following DHCP filtering configuration for untrusted ports:

- DHCP snooping is enabled on all VLANs (**service dhcp-snooping** command on page 56.24, **ip dhcp snooping** command on page 56.9)
- ARP security (**arp security** command on page 56.2) is enabled on all VLANs
- MAC address verification is enabled on the switch (**ip dhcp snooping verify mac-address** command on page 56.21; enabled by default), and all DHCP clients are directly connected to the switch.
- Access Control Lists allow IP packets that match the source IP address and MAC address of a valid lease entry in the DHCP snooping database, and deny other IP packets (**access-list** commands in **Chapter 37, IPv4 Hardware Access Control List (ACL) Commands**).
- DHCP requests containing DHCP Relay Agent Option 82 info are not allowed (**ip dhcp snooping agent-option allow-untrusted** command on page 56.11).
- Log messages and SNMP notifications are enabled for DHCP snooping and ARP security violations (**ip dhcp snooping violation** command on page 56.22, **arp security violation** command on page 56.3, **snmp-server enable trap** command on page 67.18).

Table 55-1: DHCP filtering on the switch

When the switch ...	and ...	then the switch ...
DHCP packets		
Receives a DHCP BOOTP packet on a trusted port		Forwards the DHCP packet.
	The packet contains a valid IP address lease for a client, and the maximum number of leases for the client port has not been reached.	Adds or updates a lease entry in the DHCP snooping database.
	The maximum number of leases for the client port has been reached.	Drops the DHCP packet, generates a log message for the violation, generates an SNMP notification (trap), and does not add a lease entry to the database.
A lease entry in the DHCP snooping database expires		Removes the expired entry from the database.
Receives a DHCP BOOTP request packet on an untrusted port	The source MAC address and client hardware address do not match.	Drops the packet, generates a log message for the violation, and sends an SNMP notification (trap).
Receives a DHCP BOOTP request packet on an untrusted port	The packet contains DHCP Relay Agent Option 82 info.	Drops the DHCP packet, generates a log message for the violation, and sends an SNMP notification (trap).
Receives a DHCP BOOTP reply packet on an untrusted port		Drops the DHCP packet, generates a log message for the violation, and sends an SNMP notification (trap).
IP packets		
Receives an IP packet on a trusted port		Forwards the IP packet.
Receives an IP packet on an untrusted port	Its source MAC address, IP address, and receiving port match a valid lease entry in the DHCP snooping database.	Forwards the IP packet.
Receives an IP packet on an untrusted port	Its source MAC address, IP address, and receiving port do not match a valid lease entry in the DHCP snooping database.	Drops the packet. Does not generate a log message or an SNMP notification.
ARP packets		
Receives an ARP request on a trusted port		Forwards the ARP packet.
Receives an ARP request on an untrusted port	Its source MAC address, IP address, and receiving port match a valid entry in the DHCP snooping database	Forwards the ARP packet.
Receives an ARP request on an untrusted port	Its source MAC address, IP address, and receiving port do not match an entry in the DHCP snooping database	Drops the packet, generates a log message for the violation, and sends an SNMP notification (trap).

ARP Security

ARP security prevents ARP spoofing. ARP spoofing occurs when devices send fake, or 'spoofed', ARP messages to an Ethernet LAN. This makes it possible for an unauthorized host to claim to be an authorized host. The unauthorized host can then intercept traffic intended for the authorized host, and can access the wider network.

Spoofed ARP messages contain the IP address of an authorized host, with a MAC address which does not match the real MAC address of the host. When ARP security is enabled for DHCP snooping, the switch checks ARP packets sourced from untrusted ports against the entries in the DHCP snooping binding database. If it finds a matching entry, it forwards the ARP packet as normal. If it does not find a matching entry, it drops the ARP packet. This ensures that only trusted clients (with a recognized IP address and MAC address) can generate ARP packets into the network. ARP security is not applied to packets received on trusted ports.

ARP security is disabled by default, and can be enabled on VLANs to ensure that on untrusted ports, only trusted clients (with a recognized IP address and MAC address) can generate ARP packets into the network. ARP security is applied to both dynamic and static DHCP snooping entries. For static DHCP entries without a MAC address defined, ARP security compares only the IP address details.

MAC Address Verification

When MAC address verification is enabled, the switch forwards DHCP packets received on untrusted ports only if the source MAC address and client hardware address match. MAC address verification is enabled by default.

DHCP Snooping Violations

Packets violating DHCP snooping or ARP security checks (if these are enabled) are automatically dropped. The switch can also be configured to send SNMP notifications (atDhcpsnTrap and atArpsecTrap), to generate log messages, or to shut down the link on which the packet was received.

If the switch is configured to send notifications for DHCP snooping or ARP security violations, the rate is limited to one notification per second. If there are any further violations within a second, no notifications are sent for them. After one second, the switch only sends further notifications if the source MAC address and/or the violation reason are different from previous notifications. (If log messages are also generated for ARP security and DHCP snooping violations, you can see a record of all violations in the log, even if notifications were not sent for all of them.)

Interactions with Other Features

DHCP snooping interacts with other switch features as follows:

- **Ports in trunk mode**

  The DHCP snooping feature is enabled or disabled per VLAN, and several of the related configuration settings are applied to ports. If there are multiple VLANs on a port, all the VLANs will be subject to the same per-port settings.

- **DHCP snooping can be configured with port provisioning**.

- **Authentication**

  DHCP snooping cannot be enabled on a switch that is configured for web authentication (**auth-web enable** command on page 43.35), roaming authentication (**auth roaming enable** command on page 43.19, **auth roaming disconnected** command on page 43.17), or guest VLAN authentication (**auth guest-vlan** command on page 43.9), or vice versa.

- **Stacking**

  If DHCP snooping is enabled in a stack, the DHCP snooping database and its backup file are automatically synchronized across all stack members, so that a new stack master can reinstate this database.

- **Link aggregators**

  DHCP snooping can operate over switch ports, and over static and dynamic (LACP) link aggregators (channel groups). If a switch port is added to an aggregator, DHCP snooping configuration is applied to the aggregator; configuration of the original switch port is not preserved. If the switch port is then removed from the aggregator, it returns to default DHCP snooping settings.

- **Private VLANs**

  Private VLANs are not supported for DHCP snooping.

Configuration

This section provides a general configuration procedure for DHCP snooping.

Configure DHCP Snooping

Note that if a port in trunk mode has multiple VLANs attached, then the DHCP snooping configuration settings for the port apply to all the VLANs.

Table 55-2: General configuration procedure for DHCP snooping

Step 1. Enable DHCP snooping		
1.	`awplus#` `configure terminal`	Enter Global Configuration mode.
2.	`awplus(config)#` `service dhcp-snooping`	Enable DHCP snooping on the switch. Default: disabled
3.	`awplus(config)#` `interface <vid-list>`	Enter Interface Configuration mode for the VLANs to enable DHCP snooping on.
4.	`awplus(config-if)#` `ip dhcp snooping`	Enable DHCP snooping on these VLANs. Default: disabled
5.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
6.	`awplus(config-if)#` `interface <port-list>`	Enter Interface Configuration mode for ports connected to the trusted network. The port(s) connected to the DHCP server(s) must be configured as trusted ports.
7.	`awplus(config-if)#` `ip dhcp snooping trust`	Set these ports to be trusted ports. Default: untrusted
8.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
9.	`awplus(config)#` `interface <port-list>`	If you want to allow more than one DHCP lease for any ports, enter Interface Configuration mode for the required ports. The default is likely to be suitable for edge ports; on an aggregation switch, you may need to increase the maximum number of leases for ports connected to other switches and/or for multiple VLANs. Note that you cannot change this setting once DHCP snooping ACLs are attached to these interfaces.

Table 55-2: General configuration procedure for DHCP snooping(cont.)

10.	`awplus(config-if)#` `ip dhcp snooping max-bindings <0-520>`	Change the maximum number of leases for these ports. Default: 1
11.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
Step 2. Configure DHCP filtering		
12.	`awplus(config)#` `access-list hardware <name>`	Create a hardware access list, and enter Hardware Access List Configuration mode to configure it. See the **access-list hardware (named)** command on page 37.18.

13.	`awplus(config-ip-hw-acl)#`
	`[<seqnum>] permit ip dhcpsnooping any`
	`[<seqnum>] deny ip any any`
		Configure the hardware access list to permit traffic with *source IP address* matching valid entries in the DHCP snooping database, and to deny other traffic. (The last filter applied to the ports by any access list must be the filter that denies all other traffic.)
		OR

	`awplus(config-ip-hw-acl)#`
	`[<seqnum>] permit mac dhcpsnooping any`
	`[<seqnum>] deny mac any any`
		Configure the hardware access list to permit traffic with *source MAC address* matching valid entries in the DHCP snooping database, and to deny other traffic. (The last filter applied to the ports by any access list must be the filter that denies all other traffic.)
		See the **(access-list hardware IP protocol filter)** command on page 37.23.

14.	`awplus(config-ip-hw-acl)#` `exit`	Return to Global Configuration mode.
15.	`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for the ports to add the DHCP snooping access list to. Typically this would be all untrusted ports.
16.	`awplus(config-if)#` `access-group <name>`	Add the hardware-based access list(s) to these ports. The *name* in this command is the name of the access list specified in **Step 12**.
17.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.

Table 55-2: General configuration procedure for DHCP snooping(cont.)

Step 3. Configure ARP security		
18.	`awplus(config)#` `interface <vid-list>`	Enter Interface Configuration mode for the VLANs to enable ARP security on. Default: disabled
19.	`awplus(config-if)#` `arp security`	Enable ARP security on particular VLANs if required. On untrusted ports, ARP security forwards ARP packets that have a source IP address and MAC address matching a dynamic entry in the DHCP snooping database, or an IP address matching a static entry. It drops other ARP packets, and treats them as ARP security violations. Default: disabled
20.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
Step 4. Configure DHCP Relay Agent Option 82		
21.	`awplus(config)#` `no ip dhcp snooping agent-option`	If you do not want the switch to insert DHCP Relay Agent Option 82 information into DHCP packets received on untrusted ports, or to remove this information from DHCP packets transmitted on untrusted ports, disable the DHCP Relay Agent Option 82 agent option. Default: enabled if DHCP snooping is enabled.
22.	`awplus(config)#` `ip dhcp snooping agent-option allow-untrusted`	If there are edge switches that add the DHCP Relay Agent Option 82 information to DHCP packets, and that are connected to untrusted ports on this switch, you may wish to enable this switch to forward these packets, and the associated DHCP reply packets, without changing the DHCP Relay Agent Option 82 information in them. Default: disabled.
23.	`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for one or more ports to add a Subscriber ID for.
24.	`awplus(config-if)#` `ip dhcp snooping subscriber-id [<sub-id>]`	Add the Subscriber ID for these ports. The Subscriber ID is included in DHCP Relay Agent Option 82 information. Default: no Subscriber ID.

Table 55-2: General configuration procedure for DHCP snooping(cont.)

25.	`awplus(config)#` `interface <interface-list>`	Enter Interface Configuration mode for one or more VLANs to add a Circuit ID for.
26.	`awplus(config-if)#` `ip dhcp snooping agent-option circuit-id vlantriplet`	Specify the Circuit ID for the VLAN or group of VLANs as the VLAN ID and port number. Default: VLAN ID and Ifindex number.
27.	`awplus(config)#` `interface <interface-list>`	Enter Interface Configuration mode for one or more VLANs to add a Remote ID for.
28.	`awplus(config-if)#` `ip dhcp snooping agent-option remote-id <remote-id>`	Specify the Remote ID for the VLAN or group of VLANs as an alphanumeric (ASCII) string, 1 to 63 characters in length. Default: the switch's MAC address.
29.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
Step 5. Configure MAC address verification		
30.	`awplus(config)#` `no ip dhcp snooping verify mac-address`	If not required, disable MAC address verification. Default: enabled
Step 6. Configure the DHCP snooping database		
31.	`awplus(config)#` `ip dhcp snooping database {nvs|flash}`	If required, change the location of the file to which the switch writes the dynamic entries from the DHCP snooping database. Default: nvs (non-volatile storage)
32.	`awplus(config)#` `no ip dhcp snooping delete-by-client`	By default, the switch deletes DHCP lease entries from the DHCP snooping database when it receives matching DHCP release messages. Disable these deletions if required, so that lease entries remain in the database until they expire. Default: enabled—entries are deleted when leases are released.
33.	`awplus(config)#` `ip dhcp snooping delete-by-linkdown`	If required, set the switch to delete dynamic entries from the DHCP snooping database when their ports go down. Default: disabled—entries remain if links go down.

Table 55-2: General configuration procedure for DHCP snooping(cont.)

34.	`awplus(config)#` `ip source binding <ipaddr> [<macaddr>] vlan <vid> interface <port>`	You can actively add, modify, or remove static entries from the DHCP snooping database.
35.	`awplus#` `ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid> interface <port> expiry <expiry-time>`	You can actively add or remove dynamic entries from the DHCP snooping database. These changes affect the current database and backup file, but are not stored in the running configuration.
Step 7. Configure violation actions		
36.	`awplus(config)#` `interface <port-list>`	Enter Interface Configuration mode for the ports for which you want to configure actions in response to DHCP snooping or ARP security violations.

37.	`awplus(config-if)#`
	`ip dhcp snooping violation {log|trap|link-down} ...`
	`arp security violation {log|trap|link-down} ...`
		If required, set the switch to generate an SNMP notification (trap), to generate a log message, and/or to block traffic on the port on which a DHCP snooping and/or ARP security violation is detected.
		Default: By default, if a packet does not match the DHCP snooping and ARP security restrictions, the packet is dropped, but no other action is taken.

38.	`awplus(config-if)#` `exit`	Return to Global Configuration mode.
39.	`awplus(config)#` `snmp-server enable trap dhcpsnooping`	In order to send SNMP notifications: ■ set the action for violations to trap (**Step 37**) ■ configure SNMP—see **Chapter 67, SNMP Commands** ■ set the SNMP server to enable DHCP snooping notifications (by default notifications are disabled on the SNMP server). The port connecting the switch to the SNMP manager should be set as a trusted port (**Step 7 on page 55.10**).
40.	`awplus(config)#` `exit`	Return to Privileged Exec mode.

Table 55-2: General configuration procedure for DHCP snooping(cont.)

Step 8.	**Check the configuration**	

41.	`awplus#`
	`show ip dhcp snooping`
	`show ip dhcp snooping interface [<port-list>]`
	`show ip dhcp snooping acl`
	`show arp security`
	`show arp security interface [<port-list>]`
	`show running-config dhcp`
		Check the DHCP snooping configuration.

Step 9.	**Troubleshooting DHCP snooping**	
42.	`awplus#` `show ip dhcp snooping binding`	Check all entries in the DHCP snooping database.
43.	`awplus#` `show ip source binding`	Check the static entries in the DHCP snooping database.

44.	`awplus#`
	`show ip dhcp snooping statistics [detail] [interface <interface-list>]`
	`clear ip dhcp snooping statistics [interface <port-list>]`
		Check DHCP snooping statistics.

45.	`awplus#`
	`show arp security statistics [detail] [interface <port-list>]`
	`clear arp security statistics [interface <port-list>]`
		Check ARP security statistics.

46.	`awplus#`
	`debug ip dhcp snooping {all|acl|db|packet [detail]}`
	`show debugging ip dhcp snooping`
	`debug arp security`
	`show debugging arp security`
		Enable debug output for DHCP snooping and/or ARP security.

47.		If you have not already set the switch to log DHCP snooping and ARP security violations, you can do this for troubleshooting purposes. See **Step 37 on page 55.14**.
48.	`awplus#` `show log`	Display the contents of the buffered log, including any DHCP snooping log and debug messages. (See also **Chapter 10, Logging Commands**.)

Disabling DHCP Snooping

If you disable DHCP snooping on the whole switch (**no service dhcp-snooping** command on page 56.24), all the DHCP snooping configuration is removed, except for the Access Control Lists (ACL). Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping either on the whole switch or on particular VLANs (**no ip dhcp snooping** command on page 56.9), you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (**no access-group** command on page 37.4).

Related Features

In addition to configuring DHCP snooping as described in **Table 55-2**, consider whether you also need to configure the following:

- VLANs—see **Chapter 16, VLAN Introduction** and **Chapter 17, VLAN Commands**
- Additional ACL filters—see **Chapter 36, Access Control Lists Introduction** and **Chapter 38, IPv4 Software Access Control List (ACL) Commands**
- QoS—see **Chapter 40, Quality of Service (QoS) Introduction** and **Chapter 41, QoS Commands**
- SNMP—**Chapter 66, SNMP Introduction** and **Chapter 67, SNMP Commands**

Chapter 56: DHCP Snooping Commands

Command List 56.2
arp security 56.2
arp security violation 56.3
clear arp security statistics 56.4
clear ip dhcp snooping binding 56.5
clear ip dhcp snooping statistics 56.6
debug arp security 56.7
debug ip dhcp snooping 56.8
ip dhcp snooping 56.9
ip dhcp snooping agent-option 56.10
ip dhcp snooping agent-option allow-untrusted 56.11
ip dhcp snooping agent-option circuit-id vlantriplet 56.12
ip dhcp snooping agent-option remote-id 56.13
ip dhcp snooping binding 56.14
ip dhcp snooping database 56.15
ip dhcp snooping delete-by-client 56.16
ip dhcp snooping delete-by-linkdown 56.17
ip dhcp snooping max-bindings 56.18
ip dhcp snooping subscriber-id 56.19
ip dhcp snooping trust 56.20
ip dhcp snooping verify mac-address 56.21
ip dhcp snooping violation 56.22
ip source binding 56.23
service dhcp-snooping 56.24
show arp security 56.26
show arp security interface 56.27
show arp security statistics 56.28
show debugging arp security 56.30
show debugging ip dhcp snooping 56.31
show ip dhcp snooping 56.32
show ip dhcp snooping acl 56.33
show ip dhcp snooping agent-option 56.35
show ip dhcp snooping binding 56.36
show ip dhcp snooping interface 56.37
show ip dhcp snooping statistics 56.39
show ip source binding 56.42

Command List

This chapter gives detailed information about the commands used to configure DHCP snooping. For detailed descriptions of related ACL commands, see **Chapter 37, IPv4 Hardware Access Control List (ACL) Commands**. For more information about DHCP snooping, see **Chapter 55, DHCP Snooping Introduction and Configuration**.

DHCP snooping can operate on static link aggregators (e.g. sa2) and dynamic link aggregators (e.g. po2), as well as on switch ports (e.g. port1.0.2).

arp security

Use this command to enable ARP security on untrusted ports in the VLANs, so that the switch only responds to/forwards ARP packets if they have recognized IP and MAC source addresses.

Use the **no** variant of this command to disable ARP security on the VLANs.

Syntax

```
arp security
no arp security
```

Default Disabled

Mode Interface Configuration (VLANs)

Usage Enable ARP security to provide protection against ARP spoofing. DHCP snooping must also be enabled on the switch (**service dhcp-snooping** command on page 56.24), and on the VLANs (**ip dhcp snooping** command on page 56.9).

Example To enable ARP security on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# arp security
```

Related Commands

arp security violation
show arp security
show arp security interface
show arp security statistics

arp security violation

Use this command to specify an additional action to perform if an ARP security violation is detected on the ports. ARP security must also be enabled (**arp security** command on page 56.2).

Use the **no** variant of this command to remove the specified action, or all actions. Traffic violating ARP security will be dropped, but no other action will be taken.

Syntax

```
arp security violation {log|trap|link-down} ...
no arp security violation [log|trap|link-down] ...
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the **show log** command on page 10.37.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the **snmp-server enable trap** command on page 67.18. Notifications are limited to one per second and to one per source MAC and violation reason. Additional violations within a second of a notification being sent will not result in further notifications. Default: disabled.
`link-down`	Shut down the port that received the packet. Default: disabled.

Default When the switch detects an ARP security violation, it drops the packet. By default, it does not perform any other violation actions.

Mode Interface Configuration (switch ports, static or dynamic aggregated links)

Usage When the switch detects an ARP security violation on an untrusted port in a VLAN that has ARP security enabled, it drops the packet. This command sets the switch to perform additional actions in response to ARP violations.

If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the **no shutdown** command on page 12.15.

Example To send SNMP notifications for ARP security violations on ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# arp security violation trap
```

Related Commands

arp security
show arp security interface
show arp security statistics
show log
snmp-server enable trap

clear arp security statistics

Use this command to clear ARP security statistics for the specified ports, or for all ports.

Syntax

```
clear arp security statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The ports may be switch ports, or static or dynamic link aggregators.

Mode

Privileged Exec

Example

To clear statistics for ARP security on interface port1.0.1, use the command:

```
awplus# clear arp security statistics interface port1.0.1
```

Related Commands

arp security violation
show arp security
show arp security statistics

clear ip dhcp snooping binding

Use this command to remove one or more DHCP Snooping dynamic entries from the DHCP Snooping binding database. If no options are specified, all entries are removed from the database.

Caution

If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
clear ip dhcp snooping binding [<ipaddr>] [interface <port-list>]
   [vlan <vid-list>]
```

Parameter	Description
<ipaddr>	Remove the entry for this client IP address.
<port-list>	Remove all entries for these ports. The port list may contain switch ports, and static or dynamic link aggregators (channel groups).
<vid-list>	Remove all entries associated with these VLANs.

Mode Privileged Exec

Usage This command removes dynamic entries from the database. Note that dynamic entries can also be deleted by using the **no** variant of the **ip dhcp snooping binding** command on page 56.14.

Dynamic entries can individually restored by using the **ip dhcp snooping binding** command.

To remove static entries, use the **no** variant of the **ip source binding** command on page 56.23.

Example To remove a dynamic lease entry from the DHCP snooping database for a client with the IP address 192.168.1.2, use the command:

```
awplus# clear ip dhcp snooping binding 192.168.1.2
```

Related Commands

ip dhcp snooping binding
ip source binding
show ip dhcp snooping binding

clear ip dhcp snooping statistics

Use this command to clear DHCP snooping statistics for the specified ports, or for all ports.

Syntax `clear ip dhcp snooping statistics [interface <port-list>]`

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The port list can contain switch ports, or static or dynamic link aggregators.

Mode Privileged Exec

Example To clear statistics for the DHCP snooping on interface port1.0.1, use the command:

```
awplus# clear ip dhcp snooping statistics interface port1.0.1
```

Related Commands
clear arp security statistics
show ip dhcp snooping
show ip dhcp snooping statistics

debug arp security

Use this command to enable ARP security debugging.

Use the **no** variant of this command to disable debugging for ARP security.

Syntax

```
debug arp security
no debug arp security
```

Default Disabled

Mode Privileged Exec

Example To enable ARP security debugging, use the commands:

```
awplus# debug arp security
```

Related Commands

show debugging arp security
show log
terminal monitor

debug ip dhcp snooping

Use this command to enable the specified types of debugging for DHCP snooping.

Use the **no** variant of this command to disable the specified types of debugging.

Syntax

```
debug ip dhcp snooping {all|acl|db|packet [detail]}
no debug ip dhcp snooping {all|acl|db|packet [detail]}
```

Parameter	Description
`all`	All DHCP snooping debug.
`acl`	DHCP snooping access list debug.
`db`	DHCP snooping binding database debug.
`packet`	DHCP snooping packet debug. For the **no** variant of this command, this option also disables detailed packet debug, if it was enabled.
`detail`	Detailed packet debug.

Default Disabled

Mode Privileged Exec

Example To enable access list debugging for DHCP snooping, use the commands:

```
awplus# debug ip dhcp snooping acl
```

Related Commands

debug arp security
show debugging ip dhcp snooping
show log
terminal monitor

ip dhcp snooping

Use this command to enable DHCP snooping on one or more VLANs.

Use the **no** variant of this command to disable DHCP snooping on the VLANs.

Syntax

```
ip dhcp snooping
no ip dhcp snooping
```

Default DHCP snooping is disabled on VLANs by default.

Mode Interface Configuration (VLANs)

Usage For DHCP snooping to operate on a VLAN, it must:

- be enabled on the particular VLAN by using this command
- be enabled globally on the switch by using the **service dhcp-snooping** command on page 56.24
- have at least one port connected to a DHCP server configured as a trusted port by using the **ip dhcp snooping trust** command on page 56.20

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on particular VLANs using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (**no access-group** command on page 37.4).

Examples To enable DHCP snooping on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ip dhcp snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ip dhcp snooping
```

Related Commands

ip dhcp snooping trust
service dhcp-snooping
show ip dhcp snooping

ip dhcp snooping agent-option

Use this command to enable DHCP Relay Agent Option 82 information insertion on the switch. When this is enabled, the switch:

- inserts DHCP Relay Agent Option 82 information into DHCP packets that it receives on untrusted ports
- removes DHCP Relay Agent Option 82 information from DHCP packets that it sends to untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 insertion.

Syntax

```
ip dhcp snooping agent-option
no ip dhcp snooping agent-option
```

Default DHCP Relay Agent Option 82 insertion is enabled by default when DHCP snooping is enabled.

Mode Global Configuration

Usage DHCP snooping must also be enabled on the switch (**service dhcp-snooping** command on page 56.24), and on the VLANs (**ip dhcp snooping** command on page 56.9).

If a subscriber ID is configured for the port (**ip dhcp snooping subscriber-id** command on page 56.19), the switch includes this in the DHCP Relay Agent Option 82 information it inserts into DHCP packets received on the port.

Example To disable DHCP Relay Agent Option 82 on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping agent-option
```

Related Commands

ip dhcp snooping
ip dhcp snooping agent-option allow-untrusted
ip dhcp snooping subscriber-id
service dhcp-snooping
show ip dhcp snooping

ip dhcp snooping agent-option allow-untrusted

Use this command to enable DHCP Relay Agent Option 82 information reception on untrusted ports. When this is enabled, the switch accepts incoming DHCP packets that contain DHCP Relay Agent Option 82 information on untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 information reception on untrusted ports.

Syntax

```
ip dhcp snooping agent-option allow-untrusted
no ip dhcp snooping agent-option allow-untrusted
```

Default Disabled

Mode Global Configuration

Usage If the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports, by using this command.

When this is disabled (default), the switch treats incoming DHCP packets on untrusted ports that contain DHCP Relay Agent Option 82 information as DHCP snooping violations: it drops them and applies any violation action specified by the **ip dhcp snooping violation** command on page 56.22. The switch stores statistics for packets dropped; to display these statistics, use the **show ip dhcp snooping statistics** command on page 56.39.

Example To enable DHCP snooping Option 82 information reception on untrusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping agent-option allow-untrusted
```

Related Commands
ip dhcp snooping agent-option
ip dhcp snooping violation
show ip dhcp snooping
show ip dhcp snooping statistics

ip dhcp snooping agent-option circuit-id vlantriplet

Use this command to specify the Circuit ID sub-option of the DHCP Relay Agent Option 82 field as the VLAN ID and port number. The Circuit ID specifies the switch port and VLAN ID that the client-originated DHCP packet was received on.

Use the **no** variant of this command to set the Circuit ID to the default, the VLAN ID and Ifindex (interface number).

Syntax

```
ip dhcp snooping agent-option circuit-id vlantriplet
no ip dhcp snooping agent-option circuit-id
```

Default By default, the Circuit ID is the VLAN ID and Ifindex (interface number).

Mode Interface Configuration for a VLAN interface.

Usage The Circuit ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (**ip dhcp snooping agent-option** command on page 56.10; enabled by default), and
- DHCP snooping is enabled on the switch (**service dhcp-snooping**) and on the VLAN to which the port belongs (**ip dhcp snooping**)

Examples To set the Circuit ID to `vlantriplet` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option circuit-id
vlantriplet
```

To return the Circuit ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option circuit-id
```

Related Commands

ip dhcp snooping agent-option
ip dhcp snooping agent-option remote-id
show ip dhcp snooping
show ip dhcp snooping agent-option

ip dhcp snooping agent-option remote-id

Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field. The Remote ID identifies the device that inserted the Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the switch's MAC address.

Use the **no** variant of this command to set the Remote ID to the default, the switch's MAC address.

Syntax

```
ip dhcp snooping agent-option remote-id <remote-id>
no ip dhcp snooping agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. If the Remote ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default The Remote ID is set to the switch's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (**ip dhcp snooping agent-option** command on page 56.10; enabled by default), and
- DHCP snooping is enabled on the switch (**service dhcp-snooping**) and on the VLAN to which the port belongs (**ip dhcp snooping**)

Examples To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option remote-id
myid
```

To return the Remote ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option remote-id
```

Related Commands

ip dhcp snooping agent-option
ip dhcp snooping agent-option circuit-id vlantriplet
show ip dhcp snooping
show ip dhcp snooping agent-option

ip dhcp snooping binding

Use this command to manually add a dynamic-like entry (with an expiry time) to the DHCP snooping database. Once added to the database, this entry is treated as a dynamic entry, and is stored in the DHCP snooping database backup file. This command is not stored in the switch's running configuration.

Use the **no** variant of this command to delete a dynamic entry for an IP address from the DHCP snooping database, or to delete all dynamic entries from the database.

Caution

If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid> interface
   <port> expiry <expiry-time>

no ip dhcp snooping binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID for the entry, in the range 1 to 4094.
<port>	The port the client is connected to. The port can be a switch port, or a static or dynamic link aggregation (channel group).
<expiry-time>	The expiry time for the entry, in the range 5 to 2147483647 seconds.

Mode Privileged Exec

Usage Note that dynamic entries can also be deleted from the DHCP snooping database by using the **clear ip dhcp snooping binding** command on page 56.5.

To add or remove static entries from the database, use the **ip source binding** command on page 56.23.

Example To restore an entry in the DHCP snooping database for a DHCP client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, and with an expiry time of 1 hour, use the commands:

```
awplus# ip dhcp snooping binding 192.168.1.2 0001.0002.0003
        vlan 6 interface port1.0.6 expiry 3600
```

Related Commands

clear ip dhcp snooping binding
ip source binding
show ip dhcp snooping binding

ip dhcp snooping database

Use this command to set the location of the file to which the dynamic entries in the DHCP snooping database are written. This file provides a backup for the DHCP snooping database.

Use the **no** variant of this command to set the database location back to the default, **nvs**.

Syntax

```
ip dhcp snooping database {nvs|flash}
no ip dhcp snooping database
```

Parameter	Description
`nvs`	The switch checks the database and writes the file to non-volatile storage (NVS) on the switch at 2 second intervals if it has changed.
`flash`	The switch checks the database and writes the file to Flash memory on the switch at 60 second intervals if it has changed.

Default NVS

Mode Global Configuration

Usage If the location of the backup file is changed by using this command, a new file is created in the new location, and the old version of the file remains in the old location. This can be removed if necessary (hidden file: **.dhcp.dsn.gz**).

Example To set the location of the DHCP snooping database to non-volatile storage on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping database nvs
```

Related Commands **show ip dhcp snooping**

ip dhcp snooping delete-by-client

Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message with matching IP address, VLAN ID, and client hardware address on an untrusted port, and to discard release messages that do not match an entry in the database.

Use the **no** variant of this command to set the switch to forward DHCP release messages received on untrusted ports without removing any entries from the database.

Syntax

```
ip dhcp snooping delete-by-client
no ip dhcp snooping delete-by-client
```

Default Enabled: by default, DHCP lease entries are deleted from the DHCP snooping database when matching DHCP release messages are received.

Mode Global Configuration

Usage DHCP clients send a release message when they no longer wish to use the IP address they have been allocated by a DHCP server. Use this command to enable DHCP snooping to use the information in these messages to remove entries from its database immediately. Use the **no** variant of this command to ignore these release messages. Lease entries corresponding to ignored DHCP release messages eventually time out when the lease expires.

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when a matching release message is received, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-client
```

To set the switch to forward and ignore the content of any DHCP release messages it receives, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-client
```

Related Commands **show ip dhcp snooping**

ip dhcp snooping delete-by-linkdown

Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when its port goes down. If the port is part of an aggregated link, the entries in the database are only deleted if all the ports in the aggregated link are down.

Use the **no** variant of this command to set the switch not to delete entries when ports go down.

Syntax

```
ip dhcp snooping delete-by-linkdown
no ip dhcp snooping delete-by-linkdown
```

Default Disabled: by default DHCP Snooping bindings are not deleted when an interface goes down.

Mode Global Configuration

Usage If this command is enabled in a stack, and the master goes down and is replaced by a new master, entries in the DHCP snooping database for ports on the master are removed, unless they are part of link aggregators that are still up.

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-linkdown
```

To set the switch *not* to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-linkdown
```

Related Commands **show ip dhcp snooping**

ip dhcp snooping max-bindings

Use this command to set the maximum number of DHCP lease entries that can be stored in the DHCP snooping database for each of the ports. Once this limit has been reached, no further DHCP lease allocations made to devices on the port are stored in the database.

Use the **no** variant of this command to reset the maximum to the default, 1.

Syntax

```
ip dhcp snooping max-bindings <0-520>
no ip dhcp snooping max-bindings
```

Parameter	Description
<0-520>	The maximum number of bindings that will be stored for the port in the DHCP snooping binding database. If 0 is specified, no entries will be stored in the database for the port.

Default The default for maximum bindings is 1.

Mode Interface Configuration (port)

Usage The maximum number of leases cannot be changed for a port while there are DHCP snooping Access Control Lists (ACL) associated with the port. Before using this command, remove any DHCP snooping ACLs associated with the ports. To display ACLs used for DHCP snooping, use the **show ip dhcp snooping acl** command on page 56.33.

In general, the default (1) will work well on an edge port with a single directly connected DHCP client. If the port is on an aggregation switch that is connected to an edge switch with multiple DHCP clients connected through it, then use this command to increase the number of lease entries for the port.

If there are multiple VLANs configured on the port, the limit is shared between all the VLANs on this port. For example, the default only allows one lease to be stored for one VLAN. To allow connectivity for the other VLANs, use this command to increase the number of lease entries for the port.

Example To set the maximum number of bindings to be stored in the DHCP snooping database to 10 per port for ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# ip dhcp snooping max-bindings 10
```

Related Commands

access-group
show ip dhcp snooping acl
show ip dhcp snooping interface

ip dhcp snooping subscriber-id

Use this command to set a Subscriber ID for the ports.

Use the **no** variant of this command to remove Subscriber IDs from the ports.

Syntax

```
ip dhcp snooping subscriber-id [<sub-id>]
no ip dhcp snooping subscriber-id
```

Parameter	Description
<sub-id>	The Subscriber ID; an alphanumeric (ASCII) string 1 to 50 characters in length. If the Subscriber ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default No Subscriber ID.

Mode Interface Configuration (port)

Usage The Subscriber ID sub-option is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port if:

- a Subscriber ID is specified for the port using this command, and
- DHCP snooping Option 82 information insertion is enabled (**ip dhcp snooping agent-option** command on page 56.10; enabled by default), and
- DHCP snooping is enabled on the switch (**service dhcp-snooping**) and on the VLAN to which the port belongs (**ip dhcp snooping**)

Examples To set the Subscriber ID for port 1.0.3 to **room_534**, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# ip dhcp snooping subscriber-id room_534
```

Related Commands

ip dhcp snooping agent-option
show ip dhcp snooping interface

ip dhcp snooping trust

Use this command to set the ports to be DHCP snooping trusted ports.

Use the **no** variant of this command to return the ports to their default as untrusted ports.

Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Default All ports are untrusted by default.

Mode Interface Configuration (port)

Usage Typically, ports connecting the switch to trusted elements in the network (towards the core) are set as trusted ports, while ports connecting untrusted network elements are set as untrusted. Configure ports connected to DHCP servers as trusted ports.

Example To set switch ports 1.0.1 and 1.0.2 to be trusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# ip dhcp snooping trust
```

Related Commands **show ip dhcp snooping interface**

ip dhcp snooping verify mac-address

Use this command to verify that the source MAC address and client hardware address match in DHCP packets received on untrusted ports.

Use the **no** variant of this command to disable MAC address verification.

Syntax

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

Default Enabled—source MAC addresses are verified by default.

Mode Global Configuration

Usage When MAC address verification is enabled, the switch treats DHCP packets with source MAC address and client hardware address that do not match as DHCP snooping violations: it drops them and applies any other violation action specified by the **ip dhcp snooping violation** command on page 56.22. To bring the port back up again after any issues have been resolved, use the **no shutdown** command on page 12.15.

Example To disable MAC address verification on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping verify mac-address
```

Related Commands
ip dhcp snooping violation
show ip dhcp snooping
show ip dhcp snooping statistics

ip dhcp snooping violation

Use this command to specify the action the switch will take when it detects a DHCP snooping violation by a DHCP packet on the ports.

Use the **no** variant of this command to disable the specified violation actions, or all violation actions.

Syntax

```
ip dhcp snooping violation {log|trap|link-down} ...
no ip dhcp snooping violation [{log|trap|link-down} ...]
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the **show log** command on page 10.37. Default: disabled.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the **snmp-server enable trap** command on page 67.18. Notifications are limited to one per second and to one per source MAC and violation reason. Default: disabled.
`link-down`	Set the port status to link-down. Default: disabled.

Default By default, DHCP packets that violate DHCP snooping are dropped, but no other violation action is taken.

Mode Interface Configuration (port)

Usage If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the **no shutdown** command on page 12.15.

IP packets dropped by DHCP snooping filters do not result in other DHCP snooping violation actions.

Example To set the switch to send an SNMP notification and set the link status to link-down if it detects a DHCP snooping violation on switch ports 1.0.1 to 1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# ip dhcp snooping violation trap link-down
```

Related Commands

show ip dhcp snooping interface
show log
snmp-server enable trap

ip source binding

Use this command to add or replace a static entry in the DHCP snooping database.

Use the **no** variant of this command to delete the specified static entry or all static entries from the database.

Syntax

```
ip source binding <ipaddr> [<macaddr>] vlan <vid> interface <port>
no ip source binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address. If there is already an entry in the DHCP snooping database for this IP address, then this command replaces it with the new entry.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID associated with the entry.
<port>	The port the client is connected to.

Mode Global Configuration

Usage This command removes static entries from the database.

To remove dynamic entries, use the **clear ip dhcp snooping binding** command on page 56.5 or the **no** variant of the **ip dhcp snooping binding** command on page 56.14.

Examples To add a static entry to the DHCP snooping database for a client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, use the command:

```
awplus# configure terminal
awplus(config)# ip source binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6
```

To remove the static entry for IP address 192.168.1.2 from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding 192.168.1.2
```

To remove all static entries from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding
```

Related Commands

clear ip dhcp snooping binding
ip dhcp snooping binding
show ip dhcp snooping binding
show ip source binding

service dhcp-snooping

Use this command to enable the DHCP snooping service globally on the switch. This must be enabled before other DHCP snooping configuration commands can be entered.

Use the **no** variant of this command to disable the DHCP snooping service on the switch. This removes all DHCP snooping configuration from the running configuration, except for any DHCP snooping maximum bindings settings (**ip dhcp snooping max-bindings** command on page 56.18), and any DHCP snooping-based Access Control Lists (ACLs), which are retained when the service is disabled.

Syntax

```
service dhcp-snooping

no service dhcp-snooping
```

Default DHCP snooping is disabled on the switch by default.

Mode Global Configuration

Usage For DHCP snooping to operate on a VLAN, it must be enabled on the switch by using this command, and also enabled on the particular VLAN by using the **ip dhcp snooping** command on page 56.9.

For DHCP snooping to operate on a VLAN, it must:

- be enabled globally on the switch by using this command
- be enabled on the particular VLAN by using the **ip dhcp snooping** command on page 56.9
- have at least one port connected to a DHCP server configured as a trusted port by using the **ip dhcp snooping trust** command on page 56.20

If you disable the DHCP snooping service by using the **no** variant of this command, all DHCP snooping configuration (including ARP security, but excluding maximum bindings and ACLs) is removed from the running configuration, and the DHCP snooping database is deleted from active memory. If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (in NVS by default—see the **ip dhcp snooping database** command on page 56.15). The lease expiry times are updated.

The DHCP snooping service cannot be enabled on a switch that is configured with any of the following features, or vice versa:

- web authentication (**auth-web enable** command on page 43.35)
- roaming authentication (**auth roaming enable** command on page 43.19, **auth roaming disconnected** command on page 43.17)
- guest VLAN authentication (**auth guest-vlan** command on page 43.9).

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on the switch using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (**no access-group** command on page 37.4).

Examples To enable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# service dhcp-snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# no service dhcp-snooping
```

Related Commands

ip dhcp snooping
ip dhcp snooping database
ip dhcp snooping max-bindings
show ip dhcp snooping

show arp security

Use this command to display ARP security configuration.

Syntax `show arp security`

Mode User Exec and Privileged Exec

Example To display ARP security configuration on the switch use the command:

```
awplus# show arp security
```

Figure 56-1: Example output from the show arp security command

```
awplus# show arp security

ARP Security Information:
  Total VLANs enabled ..... 2
  Total VLANs disabled ..... 11
  vlan1 ..... Disabled
  vlan2 ..... Disabled
  vlan3 ..... Disabled
  vlan4 ..... Disabled
  vlan5 ..... Disabled
  vlan100 ..... Disabled
  vlan101 ..... Disabled
  vlan102 ..... Disabled
  vlan103 ..... Disabled
  vlan104 ..... Disabled
  vlan105 ..... Enabled
  vlan1000 ..... Disabled
  vlan1001 ..... Enabled
```

Table 56-1: Parameters in the output from the show arp security command

Parameter	Description
`Total VLANs enabled`	The number of VLANs that have ARP security enabled.
`Total VLANs disabled`	The number of VLANs that have ARP security disabled.

Related Commands
arp security
show arp security interface
show arp security statistics

show arp security interface

Use this command to display ARP security configuration for the specified ports or all ports.

Syntax `show arp security interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display ARP security information about. The port list can include switch ports, and static or dynamic aggregated links.

Mode User Exec and Privileged Exec

Example To display ARP security configuration for ports, use the command:

```
awplus# show arp security interface
```

Figure 56-2: Example output from the show arp security interface command

```
awplus#show arp security interface

Arp Security Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  KEY:  LG = Log
        TR = Trap
        LD = Link down

Port         Action
------------------------------
port1.0.1    -- -- --
port1.0.2    -- -- --
port1.0.3    LG TR LD
port1.0.4    LG -- --
port1.0.5    LG -- --
port1.0.6    LG TR --
port1.0.7    LG -- LD
...
```

Table 56-2: Parameters in the output from the show arp security interface command

Parameter	Description
`Action`	The action the switch takes when it detects an ARP security violation on the port.
`Port`	The port. Parentheses indicate that ports are configured for provisioning.
`LG, Log`	Generate a log message
`TR, Trap`	Generate an SNMP notification (trap).
`LD, Link down`	Shut down the link.

Related Commands
arp security violation
show arp security
show arp security statistics
show log
snmp-server enable trap

show arp security statistics

Use this command to display ARP security statistics for the specified ports or all ports.

Syntax `show arp security statistics [detail] [interface <port-list>]`

Parameter	Description
`detail`	Display detailed statistics.
`interface <port-list>`	Display statistics for the specified ports.

Mode User Exec and Privileged Exec

Example To display the brief statistics for the ARP security, use the command:

```
awplus# show arp security statistics
```

Figure 56-3: Example output from the show arp security statistics command

```
awplus# show arp security statistics

DHCP Snooping ARP Security Statistics:

              In          In
 Interface    Packets     Discards
---------------------------------
 port1.0.3    20          20
 port1.0.4    30          30
 port1.0.12   120         0
```

Table 56-3: Parameters in the output from the show arp security statistics command

Parameter	Description
`Interface`	A port name. Parentheses indicate that ports are configured for provisioning.
`In Packets`	The total number of incoming ARP packets that are processed by DHCP Snooping ARP Security
`In Discards`	The total number of ARP packets that are dropped by DHCP Snooping ARP Security.

Figure 56-4: Example output from the show arp security statistics detail command

```
awplus#show arp security statistics detail

DHCP Snooping ARP Security Statistics:

Interface ..................... port1.0.3
  In Packets .................. 20
  In Discards ................. 20
    No Lease .................. 20
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0

Interface ..................... port1.0.4
  In Packets .................. 30
  In Discards ................. 30
    No Lease .................. 30
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0

Interface ..................... port1.0.12
  In Packets .................. 120
  In Discards ................. 0
    No Lease .................. 0
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
```

Related Commands

arp security
arp security violation
clear arp security statistics
show arp security
show arp security interface
show log

show debugging arp security

Use this command to display the ARP security debugging configuration.

Syntax `show debugging arp security`

Mode User and Privileged Exec

Example To display the debugging settings for ARP security on the switch, use the command:

```
awplus# show debugging arp security
```

Figure 56-5: Example output from the show debugging arp security command

```
awplus# show debugging arp security

ARP Security debugging status:
  ARP Security debugging is off
```

Related Commands **arp security violation**
debug arp security

show debugging ip dhcp snooping

Use this command to display the DHCP snooping debugging configuration.

Syntax `show debugging ip dhcp snooping`

Mode User Exec and Privileged Exec

Example To display the DHCP snooping debugging configuration, use the command:

```
awplus# show debugging ip dhcp snooping
```

Figure 56-6: Example output from the show debugging ip dhcp snooping command

```
awplus# show debugging ip dhcp snooping

DHCP snooping debugging status:
  DHCP snooping debugging is off
  DHCP snooping all debugging is off
  DHCP snooping acl debugging is off
  DHCP snooping binding DB debugging is off
  DHCP snooping packet debugging is off
  DHCP snooping detailed packet debugging is off
```

Related Commands **debug ip dhcp snooping**
show log

show ip dhcp snooping

Use this command to display DHCP snooping global configuration on the switch.

Syntax `show ip dhcp snooping`

Mode User Exec and Privileged Exec

Example To display global DHCP snooping configuration on the switch, use the command:

```
awplus# show ip dhcp snooping
```

Figure 56-7: Example output from the show ip dhcp snooping command

```
DHCP Snooping Information:
  DHCP Snooping service ............. Enabled
  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Not allowed
  Binding delete by client .......... Disabled
  Binding delete by link down ....... Disabled
  Verify MAC address ................ Disabled
  SNMP DHCP Snooping trap ........... Disabled

DHCP Snooping database:
  Database location ................. nvs
  Number of entries in database ..... 2

DHCP Snooping VLANs:
  Total VLANs enabled ............... 1
  Total VLANs disabled .............. 9
  vlan1 ............. Enabled
  vlan2 ............. Disabled
  vlan3 ............. Disabled
  vlan4 ............. Disabled
  vlan5 ............. Disabled
  vlan100 ........... Disabled
  vlan101 ........... Disabled
  vlan105 ........... Disabled
  vlan1000 .......... Disabled
  vlan1001 .......... Disabled
```

Related Commands
- service dhcp-snooping
- show arp security
- show ip dhcp snooping acl
- show ip dhcp snooping agent-option
- show ip dhcp snooping binding
- show ip dhcp snooping interface

show ip dhcp snooping acl

Use this command to display information about the Access Control Lists (ACL) that are using the DHCP snooping database.

Syntax

```
show ip dhcp snooping acl

show ip dhcp snooping acl [detail|hardware] [interface
   [<interface-list>]]
```

Parameter	Description
`detail`	Detailed DHCP Snooping ACL information.
`hardware`	DHCP Snooping hardware ACL information.
`interface`	ACL Interface information.
<interface-list>	The interfaces to display information about.

Mode User Exec and Privileged Exec

Example To display DHCP snooping ACL information, use the command:

```
awplus# show ip dhcp snooping acl
```

Figure 56-8: Example output from the show ip dhcp snooping acl command

```
awplus#show ip dhcp snooping acl

DHCP Snooping Based Filters Summary:

                       Maximum   Template  Attached
Interface    Bindings  Bindings  Filters   Hardware Filters
-------------------------------------------------------------
 port1.0.1   1         520       0         0
 port1.0.2   1         3         2         6
 port1.0.3   1         2         4         8
 port1.0.4   1         2         7         14
 port1.0.5   0         2         6         12
 port1.0.6   0         1         0         0
 port1.0.7   0         1         0         0
 port1.0.8   0         1         0         0
 port1.0.9   0         1         0         0
 port1.0.10  0         1         0         0
 port1.0.11  0         1         0         0
 port1.0.12  0         1         0         0
(port2.0.1 ) 0         520       0         0
(port2.0.2 ) 0         1         0         0
```

To display DHCP snooping hardware ACL information, use the command:

```
awplus# show ip dhcp snooping acl hardware
```

Figure 56-9: Example output from the show ip dhcp snooping acl hardware command

```
awplus#show ip dhcp snooping acl hardware

DHCP Snooping Based Filters in Hardware:

Interface    Access-list(/ClassMap)        Source IP         Source MAC
-------------------------------------------------------------------------
 port1.0.2   dhcpsn1                       10.10.10.10       aaaa.bbbb.cccc
 port1.0.2   dhcpsn1                       20.20.20.20       0000.aaaa.bbbb
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 30.30.30.30       aaaa.bbbb.dddd
 port1.0.3   dhcpsn2/cmap1                 40.40.40.40       0000.aaaa.cccc
 port1.0.3   dhcpsn2/cmap1                 50.50.50.50       0000.aaaa.dddd
 port1.0.3   dhcpsn2/cmap1                 60.60.60.60       0000.aaaa.eeee
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.4   dhcpsn3/cmap2                 70.70.70.70
 port1.0.4   dhcpsn3/cmap2                 80.80.80.80
 port1.0.4   dhcpsn2/cmap1                 70.70.70.70
 port1.0.4   dhcpsn2/cmap1                 80.80.80.80
 port1.0.4   dhcpsn1                       70.70.70.70
 port1.0.4   dhcpsn1                       80.80.80.80
```

To display detailed DHCP snooping ACL information for port 1.0.4, use the command:

```
awplus# show ip dhcp snooping acl detail interface port1.0.4
```

Figure 56-10: Example output from the show ip dhcp snooping acl detail interface command

```
awplus#show ip dhcp snooping acl detail interface port1.0.4

DHCP Snooping Based Filters Information:

 port1.0.4 : Maximum Bindings ........... 2
 port1.0.4 : Template filters ........... 7
 port1.0.4 : Attached hardware filters .. 14
 port1.0.4 : Current bindings ........... 1, 1 free
 port1.0.4    Client 1 ................. 120.120.120.120
 port1.0.4 : Templates: cheese (via class-map: cmap2)
 port1.0.4 :  10 permit ip dhcpsnooping 100.0.0.0/8
 port1.0.4 : Template: dhcpsn2 (via class-map: cmap1)
 port1.0.4 :  10 permit ip dhcpsnooping any
 port1.0.4 :  20 permit ip dhcpsnooping 10.0.0.0/8
 port1.0.4 :  30 permit ip dhcpsnooping 20.0.0.0/8
 port1.0.4 :  40 permit ip dhcpsnooping 30.0.0.0/8
 port1.0.4 : Template: dhcpsn1 (via access-group)
 port1.0.4 :  10 permit ip dhcpsnooping any mac dhcpsnooping abcd.0000.0000 00
 00.ffff.ffff
 port1.0.4 : 20 permit ip dhcpsnooping any
```

Related Commands **access-list hardware (named)**
show access-list (IPv4 Hardware ACLs)

show ip dhcp snooping agent-option

Use this command to display DHCP snooping Option 82 information for all interfaces, a specific interface or a range of interfaces.

Syntax `show ip dhcp snooping agent-option [interface <interface-list>]`

Parameter	Description
`interface`	Specify the interface.
<interface-list>	The name of the interface or interface range.

Mode User Exec and Privileged Exec

Examples To display DHCP snooping Option 82 information for all interfaces, use the command:

```
awplus# show ip dhcp snooping agent-option
```

To display DHCP snooping Option 82 information for `vlan1`, use the command:

```
awplus# show ip dhcp snooping agent-option interface vlan1
```

Output **Figure 56-11: Example output from the show ip dhcp snooping agent-option command**

```
awplus#show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

  Key:      C Id = Circuit Id Format
            R Id = Remote Id
            S Id = Subscriber Id

  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Not allowed

-------------------------------------------------------------------
 vlan1       C Id = vlanifindex
             R Id = Access-Island-01-M1
 vlan2       C Id = vlantriplet
             R Id = Access-Island-01-M1
 vlan3       C Id = vlantriplet
             R Id = Access-Island-01-M3
 vlan4       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan5       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan6       C Id = vlantriplet
             R Id = 0000.cd28.074c
 port1.0.1   S Id =
 port1.0.2   S Id =
 port1.0.3   S Id = phone_1
 port1.0.4   S Id =
 port1.0.5   S Id = PC_1
 port1.0.6   S Id = phone_2
```

Related Commands
ip dhcp snooping agent-option
ip dhcp snooping agent-option circuit-id vlantriplet
ip dhcp snooping agent-option remote-id
ip dhcp snooping subscriber-id
show ip dhcp snooping
show ip dhcp snooping interface

show ip dhcp snooping binding

Use this command to display all dynamic and static entries in the DHCP snooping binding database.

Syntax `show ip dhcp snooping binding`

Mode User Exec and Privileged Exec

Example To display entries in the DHCP snooping database, use the command:

```
awplus# show ip dhcp snooping binding
```

Figure 56-12: Example output from the show ip dhcp snooping binding command

```
awplus# show ip dhcp snooping binding
DHCP Snooping Bindings:

Client           MAC              Server                        Expires
IP Address       Address          IP Address       VLAN  Port   (sec)       Type
-------------------------------------------------------------------------------
1.2.3.4          aaaa.bbbb.cccc   --               7     1.0.6   Infinite   Stat
1.2.3.6          any              --               4077  1.0.6   Infinite   Stat
1.3.4.5          any              --               1     sa1     Infinite   Stat
111.111.100.101  0000.0000.0001   111.112.1.1      1     1.0.6   4076       Dyna
111.111.101.108  0000.0000.0108   111.112.1.1      1     1.0.6   4084       Dyna
111.111.101.109  0000.0000.0109   111.112.1.1      1     1.0.6   4085       Dyna
111.211.100.101  --               --               1     1.0.2   2147483325 Dyna
111.211.100.109  00b0.0000.0009   111.112.111.111  1     1.0.2   21         Dyna
111.211.101.101  00b0.0000.0101   111.112.111.111  1     1.0.2   214        Dyna

Total number of bindings in database: 9
```

Table 56-4: Parameters in the output from the show ip dhcp snooping binding command

Parameter	Description
`Client IP`	The IP address of the DHCP client.
`MAC Address`	The MAC address of the DHCP client.
`Server IP`	The IP address of the DHCP server.
`VLAN`	The VLAN associated with this entry.
`Port`	The port the client is connected to.
`Expires (sec)`	The time in seconds until the lease expires.
`Type`	The source of the entry: ■ Dyna: dynamically entered by snooping DHCP traffic, configured by the **ip dhcp snooping binding** command, or loaded from the database backup file. ■ Stat: added statically by the **ip source binding** command
`Total number of bindings in database`	The total number of dynamic and static lease entries in the DHCP snooping database.

Related Commands
ip dhcp snooping binding
ip dhcp snooping max-bindings
show ip source binding

show ip dhcp snooping interface

Use this command to display information about DHCP snooping configuration and leases for the specified ports, or all ports.

Syntax `show ip dhcp snooping interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display DHCP snooping configuration information for. If no ports are specified, information for all ports is displayed.

Mode User Exec and Privileged Exec

Example To display DHCP snooping information for all ports, use the command:

```
awplus# show ip dhcp snooping interface
```

Figure 56-13: Example output from the show ip dhcp snooping interface command

```
awplus#show ip dhcp snooping interface

DHCP Snooping Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  Action: LG = Log
          TR = Trap
          LD = Link down

                       Full    Max
 Port         Status     Leases  Leases  Action     Subscriber-ID
-------------------------------------------------------------------------------
 port1.0.1    Untrusted  1       1       LG -- --
 port1.0.2    Untrusted  0       50      LG TR LD   Building 1 Level 1
 port1.0.3    Untrusted  0       50      LG -- --
 port1.0.4    Untrusted  0       50      LG -- --   Building 1 Level 2
 port1.0.5    Untrusted  0       50      LG -- LD   Building 2 Level 1
 port1.0.6    Untrusted  0       1       LG -- --
 port1.0.7    Untrusted  0       1       LG -- --
 port1.0.8    Untrusted  0       1       LG -- --
 port1.0.9    Untrusted  0       1       -- TR --
 port1.0.10   Untrusted  0       1       -- -- LD
 port1.0.11   Trusted    0       1       -- -- --
 port1.0.12   Trusted    0       1       -- -- --
```

Table 56-5: Parameters in the output from the show ip dhcp snooping interface command

Parameter	Description
`Port`	The port interface name.
`Status`	The port status: untrusted (default) or trusted.
`Full Leases`	The number of entries in the DHCP snooping database for the port.
`Max Leases`	The maximum number of entries that can be stored in the database for the port.
`Action`	The DHCP snooping violation actions for the port.
`Subscriber ID`	The subscriber ID for the port. If the subscriber ID is longer than 34 characters, only the first 34 characters are displayed. To display the whole subscriber ID, use the **show running-config dhcp** command on page 7.42.

Related Commands

show ip dhcp snooping
show ip dhcp snooping statistics
show running-config dhcp

show ip dhcp snooping statistics

Use this command to display DHCP snooping statistics.

Syntax `show ip dhcp snooping statistics [detail] [interface <interface-list>]`

Parameter	Description
`detail`	Display detailed statistics.
`interface <interface-list>`	Display statistics for the specified interfaces. The interface list can contain switch ports, static or dynamic link aggregators (channel groups), or VLANs.

Mode User Exec and Privileged Exec

Example To show the current DHCP snooping statistics for all interfaces, use the command:

```
awplus# show ip dhcp snooping statistics
```

Figure 56-14: Example output from the show ip dhcp snooping statistics command

```
awplus# show ip dhcp snooping statistics

DHCP Snooping Statistics:

              In            In BOOTP      In BOOTP      In
 Interface    Packets       Requests      Replies       Discards
-------------------------------------------------------------------
 vlan1        444           386           58            223
 port1.0.1    386           386           0             223
 port1.0.2    0             0             0             0
 port1.0.3    0             0             0             0
 port1.0.4    0             0             0             0
 port1.0.5    0             0             0             0
 port1.0.6    58            0             58            0
```

Figure 56-15: Example output from the show ip dhcp snooping statistics detail command

```
awplus# show ip dhcp snooping statistics detail

DHCP Snooping Statistics:

Interface ..................................... port1.0.1, All counters 0
Interface ..................................... port1.0.2, All counters 0
Interface ..................................... port1.0.3, All counters 0
Interface ..................................... port1.0.4
  In Packets .................................. 50
    In BOOTP Requests ......................... 25
    In BOOTP Replies .......................... 25
  In Discards ................................. 1
    Invalid BOOTP Information ................. 0
    Invalid DHCP ACK .......................... 0
    Invalid DHCP Release or Decline ........... 0
    Invalid IP/UDP Header ..................... 0
    Max Bindings Exceeded ..................... 1
    Option 82 Insert Error .................... 0
    Option 82 Received Invalid ................ 0
    Option 82 Received On Untrusted Port ...... 0
    Option 82 Transmit On Untrusted Port ...... 0
    Reply Received On Untrusted Port .......... 0
    Source MAC/CHADDR Mismatch ................ 0
    Static Entry Already Exists ............... 0
Interface ..................................... port1.0.5, All counters 0
Interface ..................................... port1.0.6, All counters 0
```

Table 56-6: Parameters in the output from the show ip dhcp snooping statistics command

Parameter	Description
`Interface`	The interface name.
`In Packets`	The total number of incoming packets that are processed by DHCP Snooping.
`In BOOTP Requests`	The total number of incoming BOOTP Requests.
`In BOOTP Replies`	The total number of incoming BOOTP Replies.
`In Discards`	The total number of incoming packets that have been discarded.
`Invalid BOOTP Information`	Packet contained invalid BOOTP information, such as an invalid BOOTP.OPCode.
`Invalid DHCP ACK`	A DHCP ACK message was discarded, for reasons such as missing Server Option or Lease Option.
`Invalid DHCP Release or Decline`	A DHCP Release or Decline message was discarded, for reasons such as mismatch between received interface and current binding information.
`Invalid IP/UDP Header`	A problem was detected in the IP or UDP header of the packet.
`Max Bindings Exceeded`	Accepting the packet would cause the maximum number of bindings on a port to be exceeded.
`Option 82 Insert Error`	An error occurred while trying to insert DHCP Relay Agent Option 82 information.
`Option 82 Received Invalid`	The DHCP Relay Agent Option 82 information received did not match the information inserted by DHCP Snooping.

Table 56-6: Parameters in the output from the show ip dhcp snooping statistics command(cont.)

Parameter	Description
`Option 82 Received On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was received on an untrusted port.
`Option 82 Transmit On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was to be sent on an untrusted port.
`Reply Received On Untrusted Port`	A BOOTP reply was received on an untrusted port.
`Source MAC/CHADDR Mismatch`	The L2 Source MAC address of the packet did not match the client hardware address field (BOOTP.CHADDR).
`Static Entry Already Exists`	An entry could not be added as a static entry already exists.

Related Commands

clear ip dhcp snooping statistics
ip dhcp snooping
ip dhcp snooping violation

show ip source binding

Use this command to display static entries in the DHCP snooping database. These are the entries that have been added by using the **ip source binding** command on page 56.23.

Syntax `show ip source binding`

Mode User Exec and Privileged Exec

Example To display static entries in the DHCP snooping database information, use the command:

```
awplus# show ip source binding
```

Figure 56-16: Example output from the show ip source binding command

```
awplus# show ip source binding

IP Source Bindings:

Client       MAC                              Expires
IP Address   Address          VLAN  Port        (sec)      Type
-------------------------------------------------------------------
 1.1.1.1     0000.1111.2222   1     port1.0.1   Infinite   Static
```

Table 56-7: Parameters in the output from the show ip source binding command

Parameter	Description
`Client IP Address`	The IP address of the DHCP client.
`MAC Address`	The MAC address of the DHCP client.
`VLAN`	The VLAN ID the packet is received on.
`Port`	The Layer 2 port name the packet is received on.
`Expires (sec)`	Always infinite for static bindings, or when the leave time in the DHCP message was 0xffffffff (infinite).
`Type`	DHCP Snooping binding type: Static

Related Commands
ip source binding
show ip dhcp snooping binding

Part 6: Network Availability

- Chapter 57 EPSR Introduction and Configuration
- Chapter 58 EPSR Commands
- Chapter 59 RRP Snooping Introduction and Commands

Chapter 57: EPSR Introduction and Configuration

Introduction 57.2
Ring Components and Operation 57.2
Fault Detection and Recovery 57.4
- Fault Recovery 57.4
- Restoring Normal Operation 57.5
- Managing Rings with Two Breaks 57.6
- Recovery When One Break is Restored 57.8

Configuration Examples 57.10
- Single Domain, Single Ring Network 57.10
- Single Ring, Dual Domain Network 57.16

Interconnected Rings 57.17
- Superloop Protection 57.18
- EPSR Superloop Prevention 57.19
- Configuring a Basic Superloop Protected Two Ring EPSR Network 57.22
- Sample Show Output 57.37
- Adding a New Data VLAN to a Functioning Superloop Topology 57.41
- EPSR and Spanning Tree Operation 57.44

Introduction

Ethernet Protection Switching Ring (EPSR) is a protection system that prevents loops within Ethernet ring based topologies. EPSR offers a rapid detection and recovery time (in the order of 50 ms, depending on configuration) if a link or node fails. This rapid recovery time makes EPSR a more effective alternative to spanning tree options when using ring-based topologies to create high speed resilient Layer 2 networks.

Ring Components and Operation

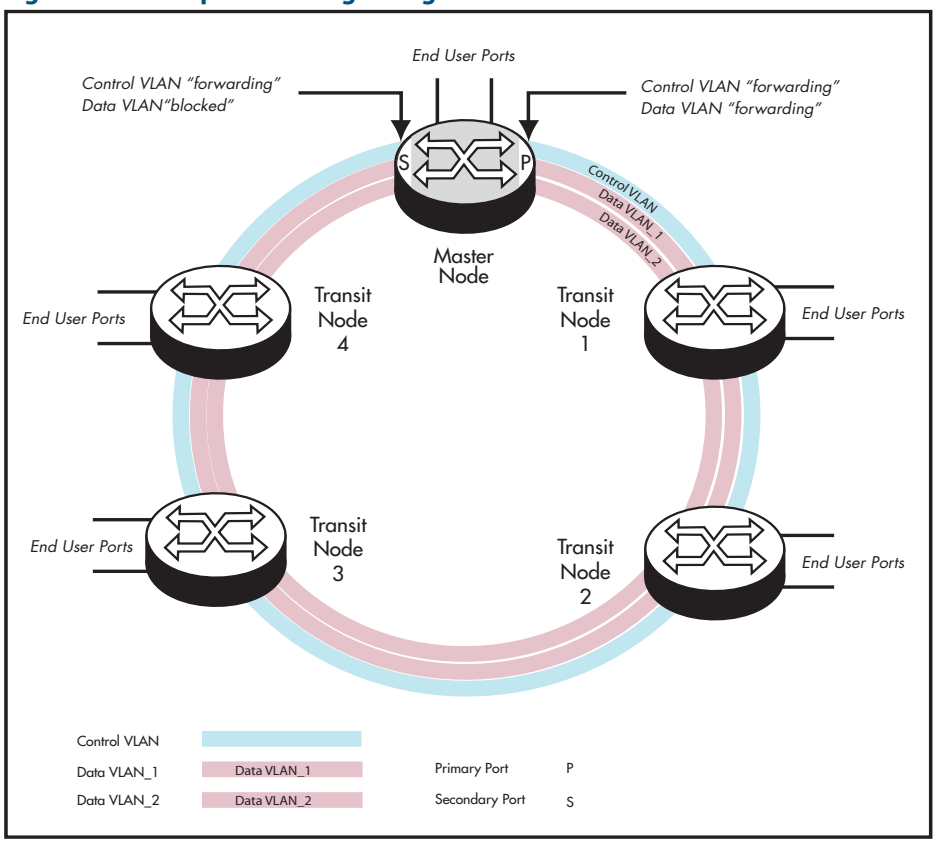
EPSR operates only on ring-based topologies. An EPSR ring comprises a series of nodes (Ethernet bridges) connected end to end. The figure below shows a basic ring configuration. A ring comprises one master node and a number of transit nodes. Each node connects to the ring via two ports. On the master node one port is configured to be the primary port and the other, the secondary port.

Note

Within an EPSRing your switch can only operate as transit node. To form an EPSR ring using switches of this type, you will need to use an alternative Allied Telesis switch, such as an x610 Series switch or an x510 Series switch (with a Premium License), to function as the master node.

In the configuration examples shown later in this chapter, master node configuration is included for completeness; however, the commands shown will need to be applied to the switch selected to be the master node.

Figure 57-1: Simple EPSR ring configuration



EPSR instances and domains

Each physical EPSR ring contains one or more EPSR domains. An EPSR instance can be thought of as a component of an EPSR ring domain that exists on a single node. A set of instances across the whole ring is called a "domain." Therefore a ring whose individual nodes each have two instances results in a two domain ring. Each instance contains a control VLAN and a number of data VLANs.

The EPSR control VLAN and its associated data VLANs form a Ring Domain. Although a physical ring can have more than one domain, each domain must operate as a separate logical group of VLANs and must have its own master node. This means that several domains may share the same physical network, but must operate as logically separate VLAN groups.

Control VLAN

The function of the control VLAN is to monitor the ring domain and maintain its operational functions. To do this it transmits and monitors operational healthcheck messages using EPSR healthcheck control frames. The control VLAN carries no user data.

Data VLAN

The data VLAN carries the user data around the ring. Several data VLANs can share a common control VLAN.

Master node

The master node controls the ring operation. It issues healthcheck messages at regular intervals from its primary port and monitors their arrival back at its secondary port - after they have circled the ring. Under normal operating conditions the master node's secondary port is always in the blocking state to all data VLAN traffic. This is to prevent data loops forming within the ring. This port however, operates in the forwarding state for the traffic on the control VLAN. Loops do not occur on the control VLAN because the control messages stop at the secondary port, having completed their path around the ring.

Note

Within an EPSRing your switch can only operate as transit node. To form an EPSR ring using switches of this type, you will need to use an alternative Allied Telesis switch, such as an x610 Series switch or an x510 Series switch (with a Premium License), to function as the master node.

In the configuration examples shown later in this chapter, master node configuration is included for completeness; however, the commands shown will need to be applied to the switch selected to be the master node.

Transit nodes

The transit nodes operate as conventional Ethernet bridges, but with the additional capability of running the EPSR protocol. This protocol requires the transit nodes to forward the healthcheck messages from the master node, and respond appropriately when a ring fault is detected. The fault condition procedure is explained in **"Fault Detection and Recovery" on page 57.4**.

Fault Detection and Recovery

EPSR uses the following methods to detect outages in a node or a link in the ring:

- Master node polling fault detection
- Transit node unsolicited fault detection

Master node polling

The master node issues healthcheck messages from its primary port as a means of checking the condition of the EPSR network ring. These messages are sent at regular periods, controlled by the **hellotime** parameter of the **epsr** command on page 58.4. A failover timer is set each time a healthcheck message leaves the master node's primary port. The timeout value for this timer is set by the **failover** parameter of the **epsr** command on page 58.4. If the failover timer expires before the transmitted healthcheck message is received by the master node's secondary port, the master node assumes that there is a fault in the ring, and implements its fault recovery procedures. Because this method relies on a timer expiry, its operation is inherently slower than the "transit node unsolicited detection method" described next.

Transit node unsolicited

Transit node unsolicited fault detection relies on transit nodes detecting faults at their interfaces, and immediately notifying master nodes about the break. When a transit node detects a connectivity loss, it sends a "links down" message over its good link. Because a link spans two nodes, both nodes send the "links down" message back to the master node. These nodes also change their state from "links up" to "links down," and change the state of the port connecting to the broken link, from "forwarding" to "blocking."

Fault Recovery

When the master node detects an outage in the ring by using its detection methods, it does the following:

1. Declares the ring to be in a "failed" state.
2. Unblocks its secondary port to enable the data VLAN traffic to pass between its primary and secondary ports.
3. Flushes its own forwarding database (FDB) for (only) the two ring ports.
4. Sends an EPSR Ring-Down-Flush-FDB control message to all the transit nodes, via both its primary and secondary ports.

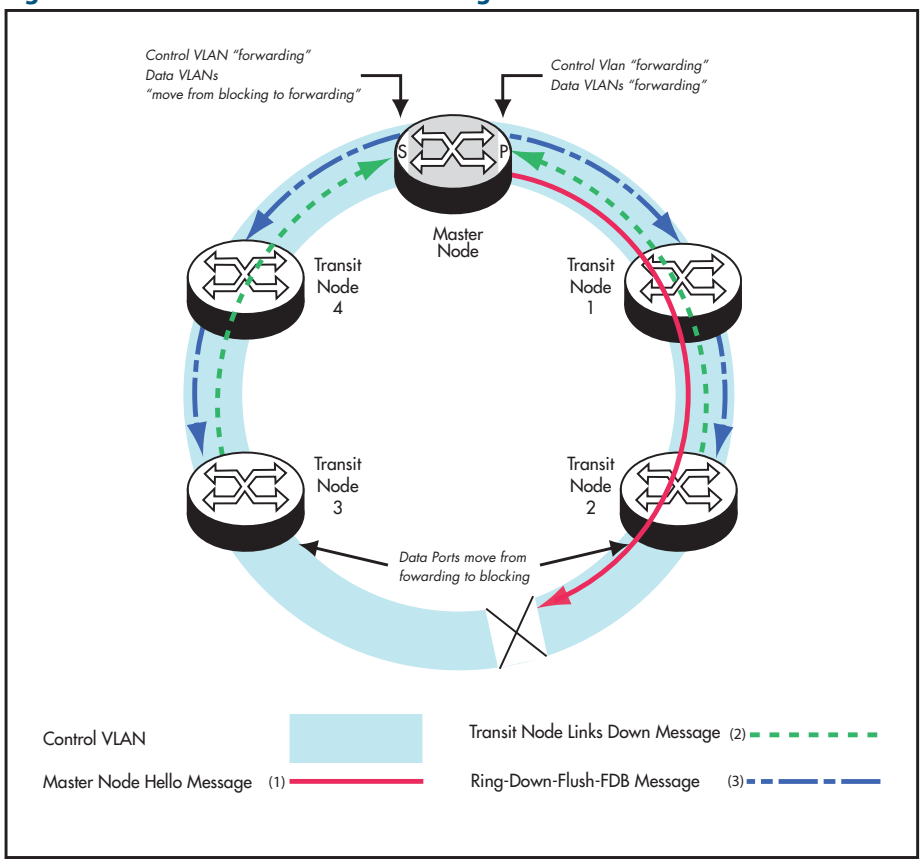
Transit nodes respond to the Ring-Down-Flush-FDB message by flushing their forward databases for each of their ring ports. As the data starts to flow in the ring's new configuration, each of the nodes (master and transit) re-learn their Layer 2 addresses. During this period, the master node continues to send health check messages over the control VLAN. This situation continues until the faulty link or node is repaired. For a multi-domain ring, this process occurs separately for each domain within the ring.

Note

When VCStack is used with EPSR, the EPSR **failovertime** must be set to at least 5 seconds to avoid any broadcast storms during failover. Broadcast storms may occur if the switch cannot failover quickly enough before the EPSR **failovertime** expires.
See the **epsr** command for further information about the EPSR **failovertime**.
See the **reboot rolling** command for further information about VCStack failover.

The following figure shows the flow of control frames under fault conditions.

Figure 57-2: EPSR fault detection messages



Restoring Normal Operation

Transit nodes

Once a fault in the ring or node has been rectified, the transit nodes that span the previously faulty link section detect that link connectivity has returned. They then move their appropriate ring port state, from Links-Down to Pre-Forwarding, and await the Ring-Up-Flush control message from the master node.

Once these transit nodes receive the Ring-Up-Flush message, they:

- flush their forward databases for both their ring ports.
- change the state of their ports from blocking to forwarding, which allows data to flow through their previously blocked ring ports.

Note

The transit nodes do not enter the forward state until they have received the Ring-Up-Flush message. This prevents the possibility of a loop condition occurring caused by the transit nodes moving into the forwarding state before the master node secondary port can return to the blocking state. During such a period, the ring would have no ports blocked.

Master node

With the link restored, the healthcheck messages that are sent from the primary port of the master node now complete the loop and arrive at the master node's secondary port. The master node restores normal conditions as follows:

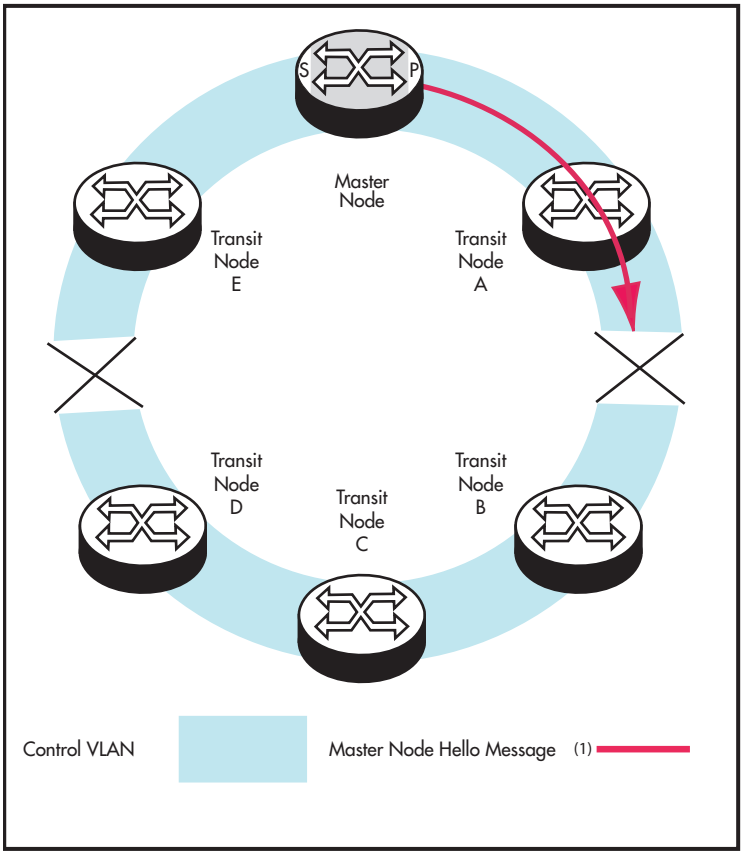
1. Declares the ring to be in a "complete" state.
2. Blocks its secondary port for data (non-control) traffic.
3. Flushes its forwarding database for its two ring ports.

4. Sends a Ring-Up-Flush-FDB message from its primary port, to all transit nodes.

Managing Rings with Two Breaks

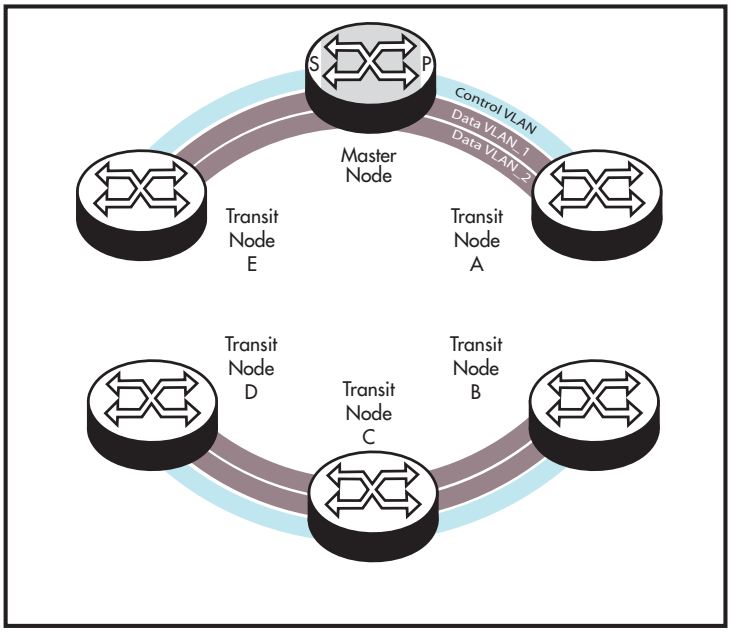
To restore a link with two breaks you need to run the EPSR Enhanced Recovery feature. Consider the network shown below:

Figure 57-3: EPSR ring with two breaks



In this situation the ring will attempt to recover as previously described in **"Fault Recovery" on page 57.4**. This will result in the split-ring operation shown in **Figure 57-4**.

Figure 57-4: EPSR split ring

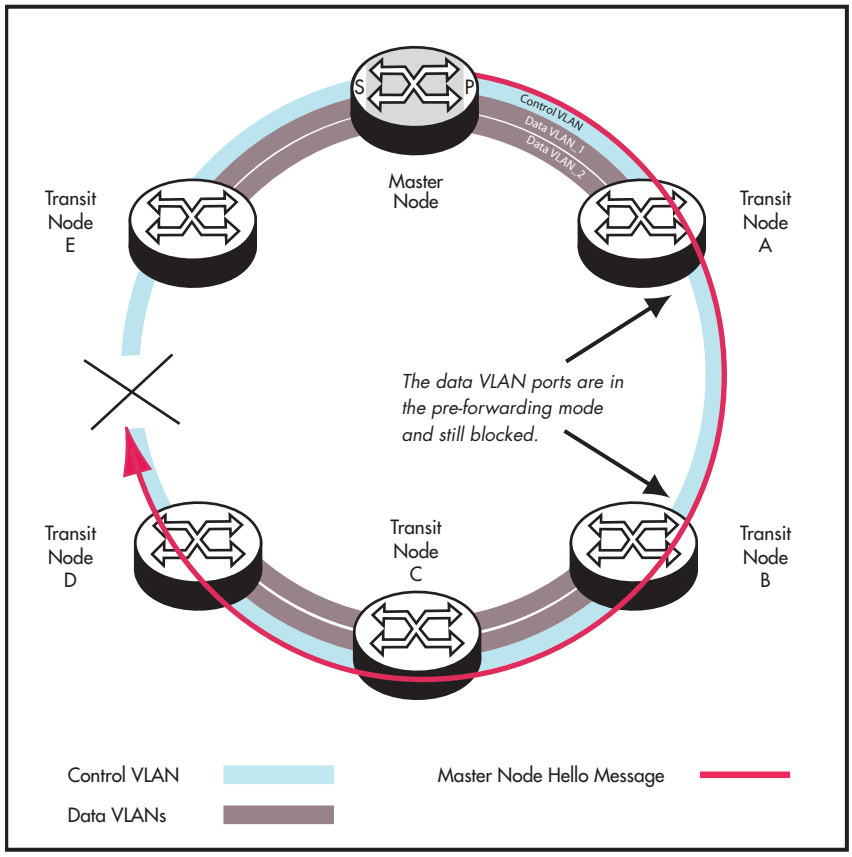


In this operational mode each portion of the ring operates as an independent link layer broadcast domain each containing the original data VLANs and control VLAN.

Recovery When One Break is Restored

Figure 57-5 on page 57.8 shows a ring with the link between nodes A and B restored. At this point the ring's behavior will depend on whether the **epsr enhancedrecovery enable** command on page 58.7 has been set.

Figure 57-5: EPSR ring with one link restored



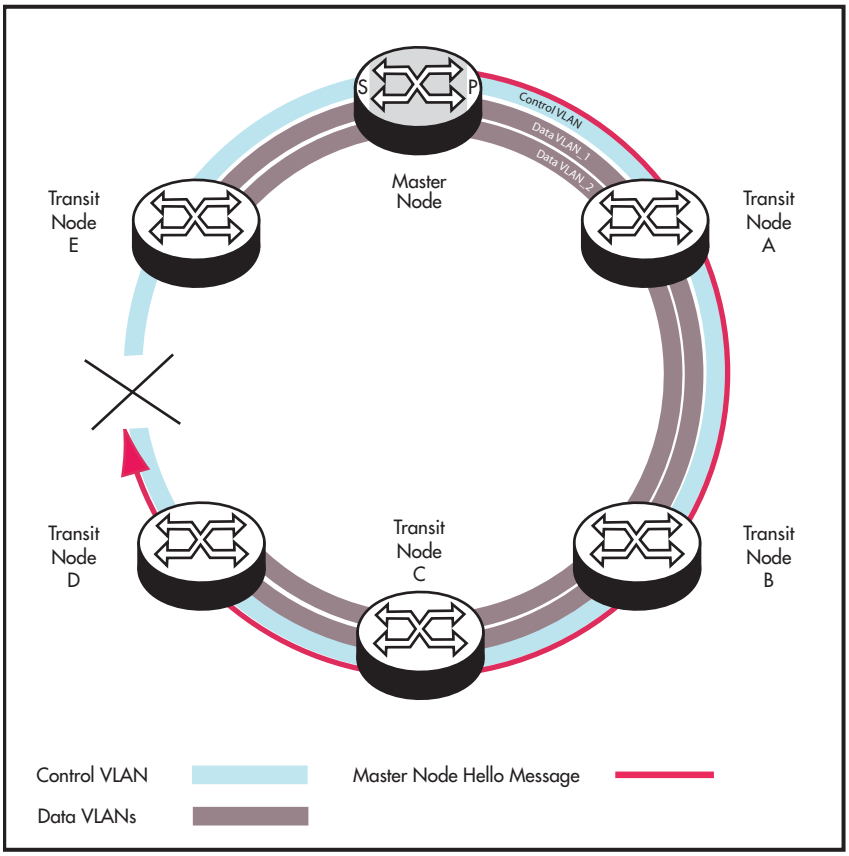
Enhanced recovery disabled

With the enhanced recovery feature disabled, the Hello messages will now reach the remaining ring break; however from a user's perspective, the ring will remain as shown in the split state shown in **Figure 57-4**.

Enhanced recovery enabled

With the enhanced recovery feature enabled, switch nodes A and B are able to detect the restored link, and will place all their ring ports in the forwarding state. Although the ring will remain in the "failed" state because of the remaining break; communication between the nodes is restored. The network then operates as shown in **Figure 57-6**.

Figure 57-6: EPSR operation in partially recovered state



Configuration Examples

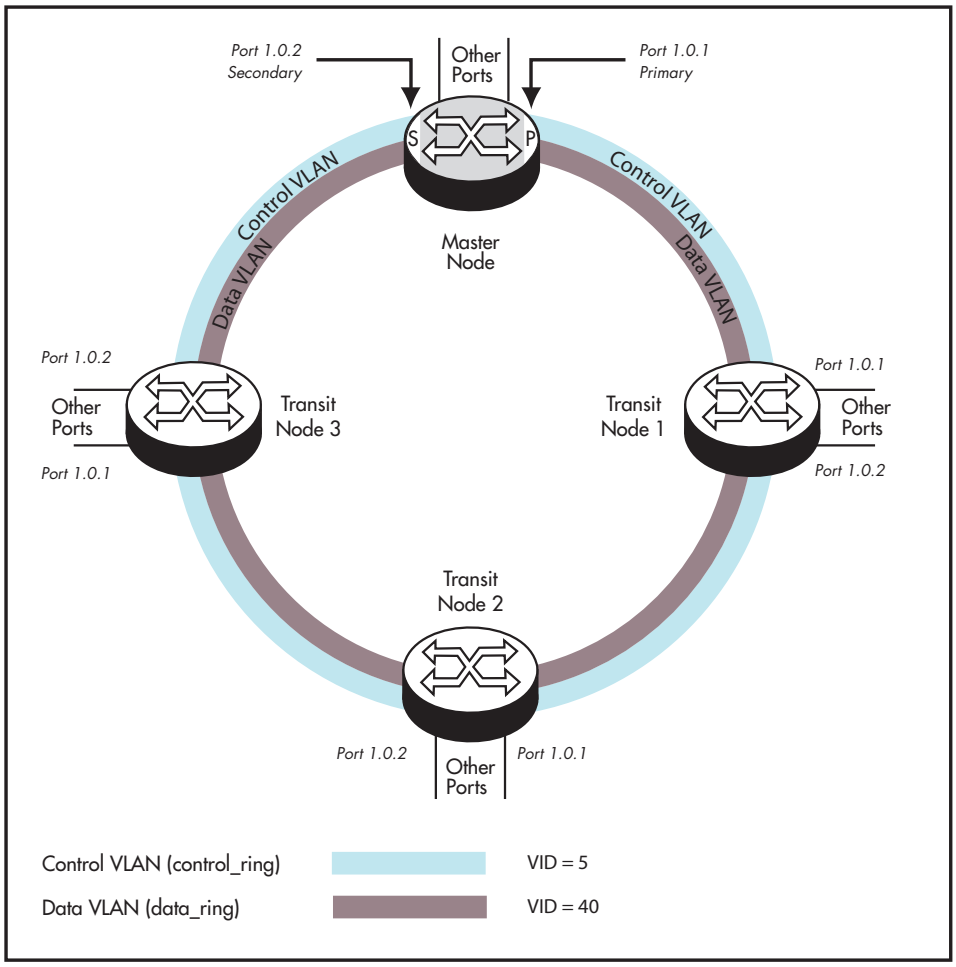
This section describes how to configure EPSR in following ways:

- **Single Domain, Single Ring Network**
- **Single Ring, Dual Domain Network**
- **EPSR and Spanning Tree Operation**

Single Domain, Single Ring Network

This example shows a simple single ring, single domain configuration with no connecting lobes.

Figure 57-7: EPSR single domain, single ring network



Configure the Master Node

Note Within an EPSRing your switch can only operate as transit node. To form an EPSR ring using switches of this type, you will need to use an alternative Allied Telesis switch, such as an x610 Series switch or an x510 Series switch (with a Premium License), to function as the master node.

In the configuration examples shown later in this chapter, master node configuration is included for completeness; however, the commands shown will need to be applied to the switch selected to be the master node.

Step 1: Create the control and data VLANs on the Master Node

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 5 name control_vlan state enable`	Enable VLAN 5 called `control_vlan` on the Master Node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data_vlan state enable`	Enable VLAN 40 called `data_vlan` on the Master Node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Add port1.0.1 to these VLANs

`awplus(config)#` `interface port1.0.1`	Specify the interface (`port1.0.1`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 5`	Enable VLAN 5 on this port.
`awplus(config-if)#` `switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#` `exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 3: Add port1.0.2 to these VLANs

`awplus(config)#` `interface port1.0.2`	Specify the interface (`port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 5`	Enable VLAN 5 on this port.
`awplus(config-if)#` `switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 4: Create the EPSR instance called “blue” on the master node; make VLAN 5 the control VLAN and port 1.0.1 the primary port

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr blue mode master controlvlan 5 primaryport port1.0.1`	Create an EPSR instance called `blue` on `vlan5`. Make `vlan5` the control VLAN. Make `port 1.0.1` the primary port. Make this node the master. Note that you can only run this command on switches that have EPSR Master capability.

Step 5: Add a data VLAN to the EPSR instance called “blue” on the Master Node

`awplus(config-epsr)#`	
`epsr blue datavlan 40`	On epsr instance called `blue` make `vlan40` the data VLAN. Note that you can only run this command on switches that have EPSR Master capability.

Step 6: Enable the EPSR instance called “blue” on the Master Node

`awplus(config-epsr)#`	
`epsr blue state enable`	Enable the EPSR instance named `blue`. Note that you can only run this command on switches that have EPSR Master capability.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Now you can configure the transit nodes.

Step 7: Create the control and data VLANs on a transit node

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 5 name control_vlan state enable`	Enable VLAN 5 called `control_vlan` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data_vlan state enable`	Enable VLAN 40 called `data_vlan` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 8: Add port1.0.1 to the VLANs

`awplus(config)#` `interface port1.0.1`	Specify the interface (`port1.0.1`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 5`	Enable VLAN 5 on this port.
`awplus(config-if)#` `switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 9: Add port1.0.2 to the VLANs

`awplus(config)#`	
`interface port1.0.2`	Specify the interface (`port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 5`	Enable VLAN 5 on this port.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 10: Create the EPSR instance called “blue” on a transit node, make VLAN 5 the control VLAN

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr blue mode transit controlvlan 5`	Create an EPSR instance called `blue` on `vlan5`. Make `vlan5` the control VLAN. Make this node a transit node.

Step 11: Add a data VLAN to the EPSR instance called “blue” on the transit node

`awplus(config-epsr)#`	
`epsr blue datavlan 40`	On the EPSR instance called `blue` make `vlan40` the data VLAN.

Step 12: Enable the EPSR instance called “blue” on the transit node

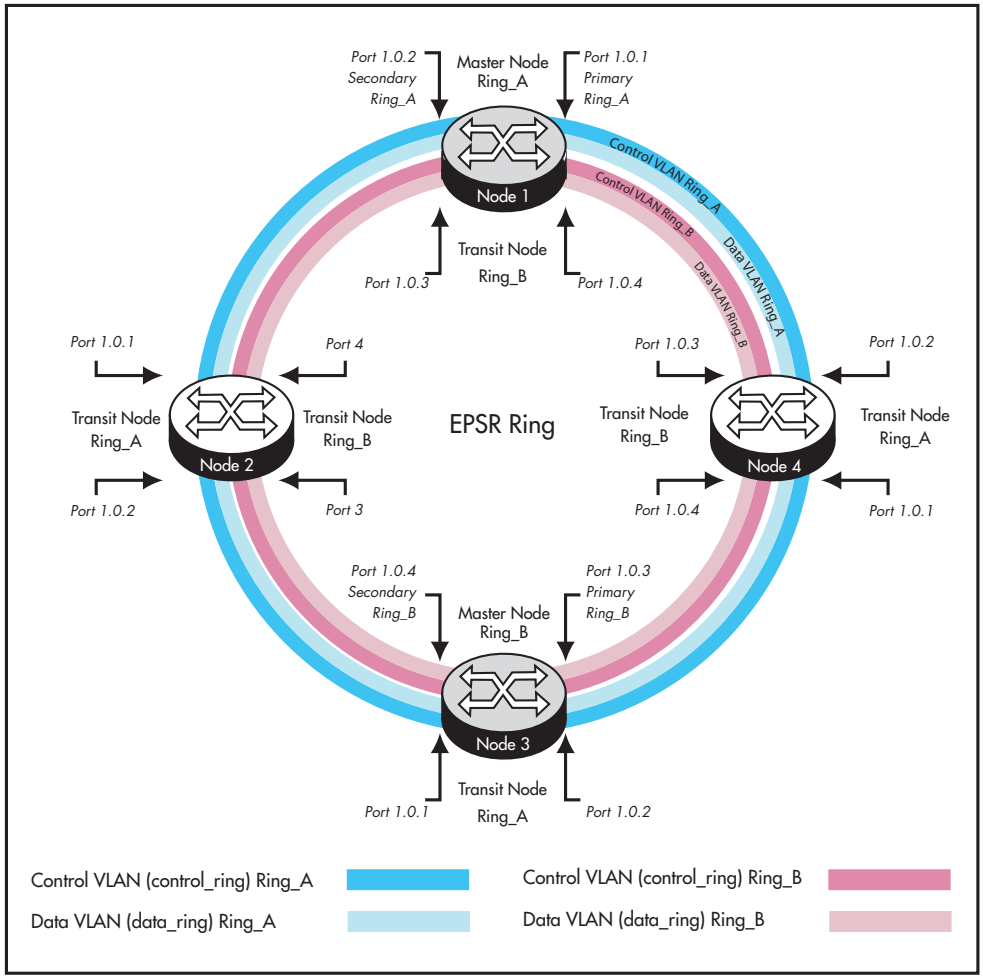
`awplus(config-epsr)#`	
`epsr blue state enable`	Enable the EPSR instance named `blue`.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Now you can use the same procedure to configure the remaining transit nodes.

Single Ring, Dual Domain Network

This example shows an EPSR configuration where two EPSR domains share the same physical ring. This configuration enables two sets of users to run totally separate Layer 2 networks. Better load distribution around the ring can be achieved by configuring different nodes to be the master for each ring.

Figure 57-8: EPSR single ring network, two domain network

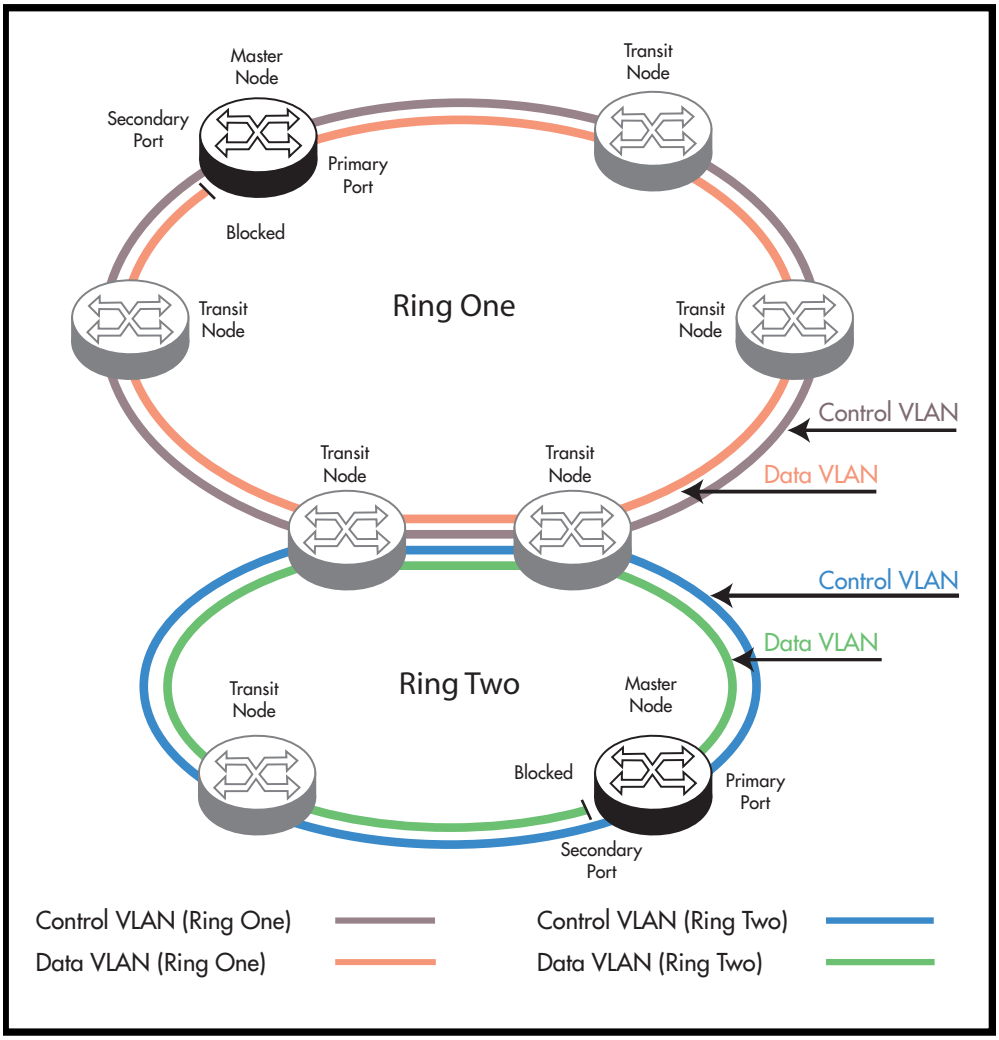


Interconnected Rings

This example shows an EPSR configuration where two rings share a common segment. This configuration will operate as two independent rings, providing that there is no data VLAN sharing between the two rings. If a break occurs in either ring then, each ring will implement its own independent recovery procedures. If a break occurs in the common segment, then each Master node will unblock its secondary port using the normal fault recovery procedure.

Where data VLANS are shared between the rings a fault condition know as “SuperLoop” can occur. The next section deals with superloops and how to manage them.

Figure 57-9: Interconnected EPSR Rings with no data VLAN sharing



Superloop Protection

Careful attention must be paid when creating EPSR networks with interconnecting links, to avoid an error condition known as superloops. This sections explains what superloops are and how to prevent them.

What is a an EPSR superloop?

An EPSR superloop is a data loop whose path traverses more than a single EPSR ring. This fault condition usually occurs when there is a break in a physical segment that is shared by the two rings. For a superloop condition to occur, the two physical rings must share some of their data VLANS. **Figure 57-10 on page 57.18**shows an EPSR ring with a superloop condition caused by a break in the common ring segment. **Figure 57-11 on page 57.19** shows the Superloop data path ring caused by the broken common ring segment. The superloop condition occurs because both rings detect the ring segment break and as a result both master nodes unblock their secondary ports.

Figure 57-10: Interconnected EPSR rings with data VLAN sharing

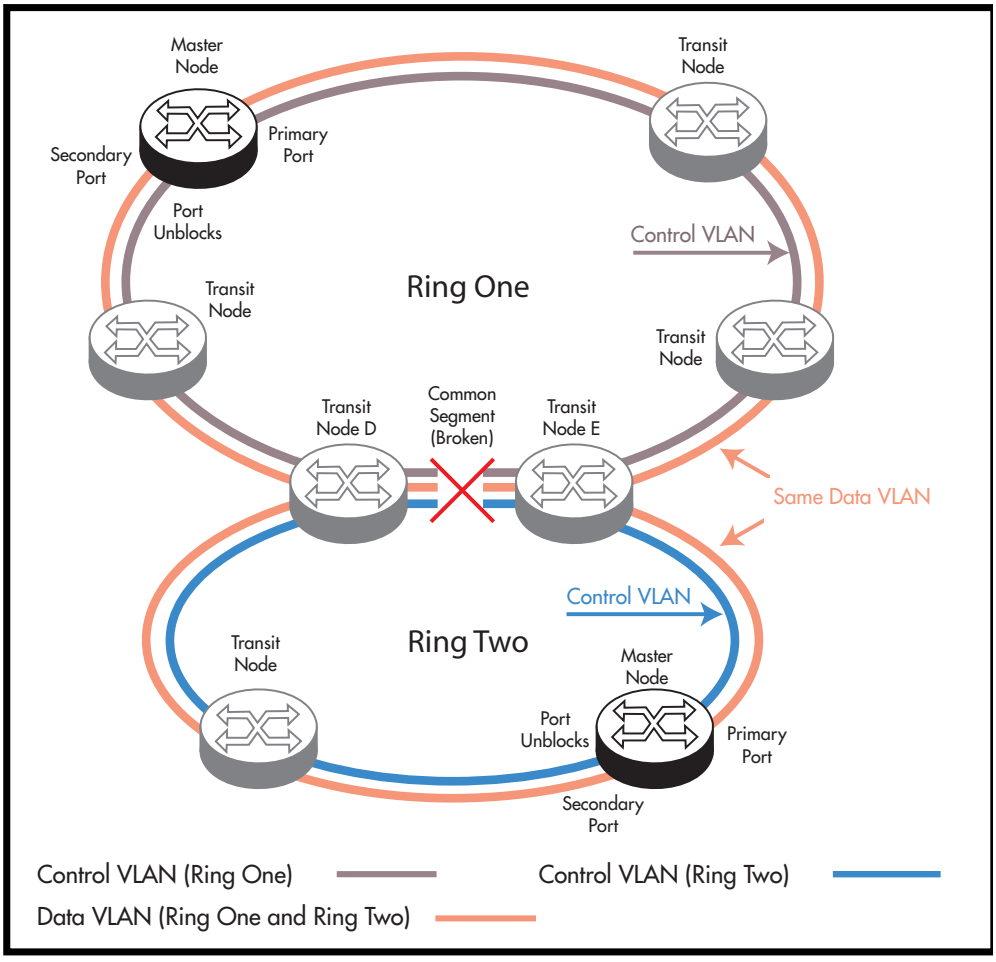
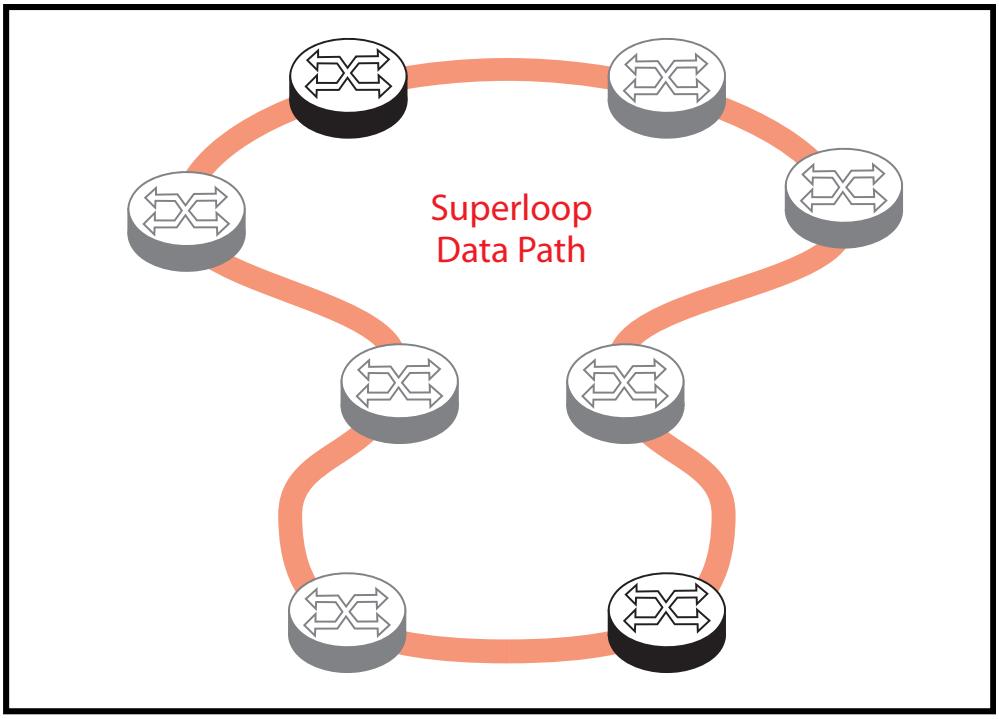


Figure 57-11: EPSR superloop data path caused by a broken common ring segment



EPSR Superloop Prevention

Alliedware Plus version 5.4.2 onwards contains mechanisms to prevent superloops forming. The Superloop prevention facility enables rings to be assigned priority level between 0 and 127, with 1 representing the lowest priority and 127 the highest. Level 0 (the default setting) applies the functionality of no Superloop prevention. Enabling superloop prevention changes the way the EPSR nodes respond under fault conditions.

Superloop prevention is enabled for an EPSR ring instance by setting the **epsr priority** command on page 58.10. Setting a priority value greater than 0 applies superloop prevention to that particular instance. How the superloop function is applied will depend on the role of the node within the ring, i.e. whether it is a master node or a transit node, and its physical location within the ring. Here is how the functions of Superloop prevention modify the nodal behavior for a particular ring instance:

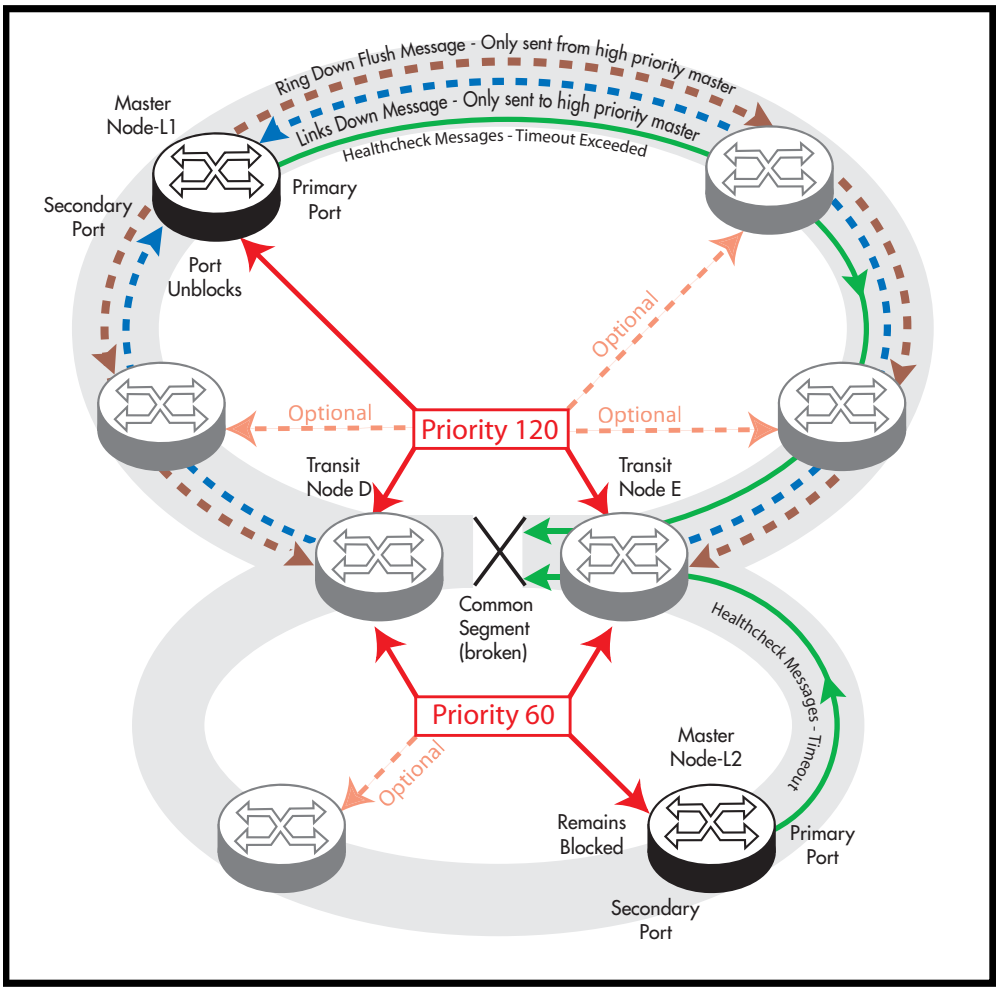
- A master node with its epsr priority set to zero will consider the superloop function to be turned off.
- A master node with its epsr priority set within the range 1-127 will consider the superloop function to be enabled, and will change its behavior in the following ways.
  - « It will **not** unblock its secondary port following the expiry of the Master Node Hello message timer. However, a ring-down-flush message will still be sent.
  - « It **will** only unblock its secondary port when it receives a Links Down message from a transit node.
- A transit node that is not connect to a shared link will be unaffected by having its epsr priority set for any of its instances.
- A transit node that is connected to a shared link will change its behavior in the following ways:
  - « It will compare its priority settings applied to each of the instances sharing the common link. So for the network of **Figure 57-10 on page 57.18** Transit Node D

will compare the priority setting for Ring One, with the priority setting for Ring Two.

If the shared link fails, the transit node will only issue a **Transit Node Links Down message** on the ring that is configured with the highest priority.

The result of these behavior changes is that when the shared link fails, only the master node located on the higher priority ring will unblock its secondary port; because this is the only master node that will receive the **Transit Node Links Down message**. Note also that the master node will receive these messages from the transit nodes at either end of the broken shared link (Nodes D and E). This concept is illustrated in the following figure.

Figure 57-12: EPSR behavior under fault conditions with superloop enabled



For this process to work certain configuration rules must be obeyed.

Configuration rules for superloop protected EPSR rings

The following configuration rules are advised when configuring EPSR rings that share one or more common segments.

- Allocate a priority order to each of the interconnected rings, with 127 being the highest priority and 1 the lowest.
- A higher priority ring can have its master node located in any position; although, where possible, avoid connecting a common segment to the secondary port of a master node.
- Do not locate the master node on a segment that is shared with a higher priority ring, but you "can" locate it on a common segment that is shared with a lower priority ring. In this situation however, the port that connects to the common segment must be configured as the primary port.

  For example, in **Figure 57-12**, the upper portion of Node D could be configured as a Master Node of the upper ring (having a priority of 120), but its lower portion must be configured as a transit node (having the lower priority of 60).
- On the transit nodes that connect to shared links, allocate the ring's priority to the ports that connect to each ring. Note that both of these nodes "must" be set to the same priority value.

Note

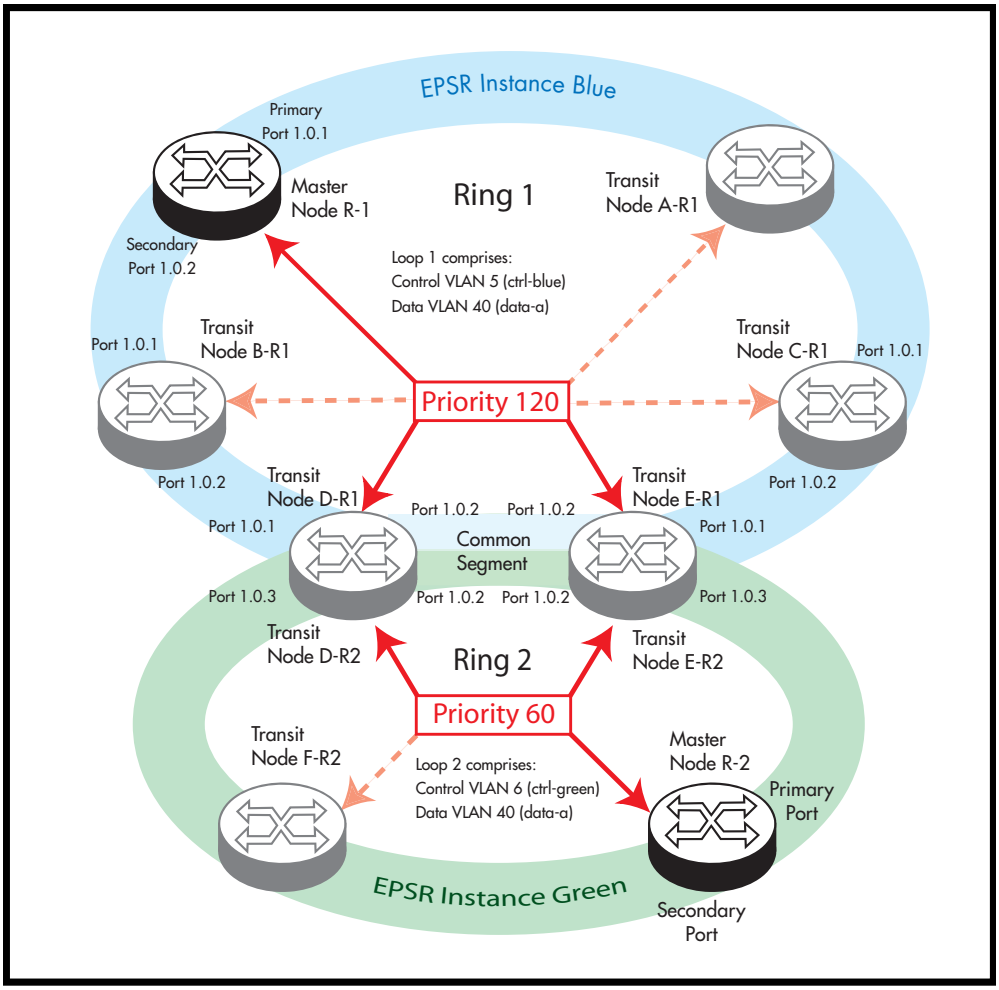
For good practice, we advise that you set all nodes within a ring to the priority assigned to that ring. So, for the network of **Figure 57-12** each of the nodes that form part of the upper ring would be configured with a priority of 120, and each of the nodes that form the lower ring would all be configured with a priority of 60.

Configuring a Basic Superloop Protected Two Ring EPSR Network

Configuration example

This section shows how to configure a basic EPSR network such as that shown in the figure below.

Figure 57-13: EPSR two shared ring example



The configuration suggested comprises the following basic steps:

- **"On Ring 1- configure the Master Node R-1" on page 57.23**
- **"On Ring 1 - configure the transit nodes A to C" on page 57.25**
- **"On Ring 2 - configure the Master Node R-2" on page 57.27**
- **"On Rings 1 and 2 - configure the Transit Nodes D and E" on page 57.29**
- **"On Ring 2 - configure the Transit Node F" on page 57.34**

Note

Within an EPSRing your switch can only operate as transit node. To form an EPSR ring using switches of this type, you will need to use an alternative Allied Telesis switch, such as an x610 Series switch or an x510 Series switch (with a Premium License), to function as the master node.

In the configuration examples shown later in this chapter, master node configuration is included for completeness; however, the commands shown will need to be applied to the switch selected to be the master node.

On Ring 1- configure the Master Node R-1

Step 1: Create the control and data VLANs (configure on the Master Node R-1)

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 5 name ctrl-blue state enable`	Enable VLAN 5 called ctrl-blue on the Master Node R-1. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data-a state enable`	Enable VLAN 40 called **data-a** on the Master Node R-1. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Add the control VLAN (ctrl-blue) to the ring ports

`awplus(config)#` `interface port1.0.1,port1.0.2`	Specify the two ring ports (`port1.0.1 and port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of these ports to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 5`	Enable VLAN 5 on these ports.
`awplus(config-if)#` `switchport trunk native vlan none`	Remove the native VLAN from these ring ports.

Step 3: Create the EPSR instance called "blue", make VLAN 5 the control VLAN and port 1.0.1 the primary port (configure on the Master Node R-1)

`awplus(config-epsr)#`	
`epsr blue mode master controlvlan 5 primaryport port1.0.1`	Create an EPSR instance called `blue` on `vlan 5`. Make `vlan 5` the control VLAN. Make `port 1.0.1` the primary port. Make this node the master.

Step 4: Add a data VLAN to the EPSR instance called "blue" (Configure on the Master Node R-1)

`awplus(config-epsr)#`	
`epsr blue datavlan 40`	On epsr instance called blue data-a the data VLAN.

Step 5: Assign a priority to the ring instance (Configure on the Master Node R-1)

`awplus(config-epsr)#`	
`epsr blue priority 120`	Set the ring instance priority to the value selected for the ring. The priority value selected is 120.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 6: Enable the EPSR instance called "blue" (configure on the Master Node R-1)

`awplus(config-epsr)#`	
`epsr blue state enable`	Enable the EPSR instance named `blue`.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 7: Add to these VLANs (configure on the Master Node R-1)

`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

On Ring 1 - configure the transit nodes A to C

Step 1: Create the control and data VLANs (on Transit Nodes A to C)

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 5 name ctrl-blue state enable`	Enable VLAN 5 called `ctrl-blue` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data-a state enable`	Enable VLAN 40 called `data-a` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Add the EPSR control vlan (ctrl-blue) to EPSR ring ports

`awplus(config)#` `interface port1.0.1,port1.0.2`	Specify the two ring ports (`port1.0.1 and port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 5`	Enable VLAN 5 on these ports.
`awplus(config-if)#` `switchport trunk native vlan none`	Remove the native VLAN from the ring ports.

Step 3: Create the EPSR instance called "blue", make VLAN 5 the control VLAN (on Transit Nodes A to C)

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr blue mode transit controlvlan 5`	Create an EPSR instance called `blue` on `vlan 5`. Make `vlan 5` the control VLAN. Make this node a transit node.

Step 4: Add a data VLAN to the EPSR instance called "blue" (on Transit Nodes A to C)

`awplus(config-epsr)#`	
`epsr blue datavlan 40`	On the EPSR instance called `blue` make `vlan 40` the data VLAN.

Step 5: Assign a priority to the ring instance (on Transit Nodes A to C)

This step is **mandatory on transit nodes that connect to a common segment**, and good practice on other transit nodes.

`awplus(config-epsr)#`	
`epsr blue priority 120`	Set the ring instance priority to the priority selected for the ring 120.

Step 6: Enable the EPSR instance called "blue" (on Transit Nodes A to C)

`awplus(config-epsr)#`	
`epsr blue state enable`	Enable the EPSR instance named `blue`.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 7: Add the physical ports 1.0.1 and 1.0.2 to VLAN 40 (on Transit Nodes A to C)

`awplus(config)#`	
`interface port1.0.1,port1.0.2`	Specify the physical ring ports (`ports1.0.1` and ports 1.0.2) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on these ports.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

On Ring 2 - configure the Master Node R-2

Step 1: Create the control and data VLANs (configure on the Master Node R-2)

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 6 name ctrl-green state enable`	Enable vlan 6 called ctrl-green on the Master Node R-2. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data-a state enable`	Enable VLAN 40 called data-a on the Master Node R-2. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Add the control VLAN (ctrl-green) to the ring ports

`awplus(config)#` `interface port1.0.1,port1.0.2`	Specify the ports (`port1.0.1 and port1.0.2`) that you are configuring, and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 6`	Enable vlan 6 on these ports.
`awplus(config-if)#` `switchport trunk native vlan none`	Remove the native VLAN from these ring ports.

Step 3: Create the EPSR instance called "green", make VLAN 6 the control VLAN and port1.0.1 the primary port (configure on the Master Node R-2)

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr green mode master controlvlan 6 primaryport port1.0.1`	Create an EPSR instance called `ctrl-green` on `vlan 6`. Make `vlan 6` the control VLAN. Make `port 1.0.1` the primary port. Make this node the master.

Step 4: Add a data VLAN to the EPSR instance "green" (configure on the Master Node R-2)

`awplus(config-epsr)#`	
`epsr green datavlan 40`	On epsr instance called green make `vlan 40` the data VLAN.

Step 5: Assign a priority to the ring instance (configure on the Master Node R-2)

This step is **mandatory on transit nodes that connect to a common segment**, and good practice on other transit nodes.

`awplus(config-epsr)#`	
`epsr green priority 60`	Set the ring instance priority to the value selected for the ring. The priority value selected is 60.

Step 6: Enable the EPSR instance called "green" (configure on the Master Node R-2)

`awplus(config-epsr)#`	
`epsr green state enable`	Enable the EPSR instance named green.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 7: Add ports 1.0.1 and 1.0.2 to these VLANs (configure on the Master Node R-2)

`awplus(config)#`	
`interface port1.0.1,port1.0.2`	Specify the ports (`port1.0.1 and port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of these ports to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

On Rings 1 and 2 - configure the Transit Nodes D and E

Step 1: Create the control and data VLANs (on Transit Nodes D and E)

`awplus#`	
`configure terminal`	Enter the Global Configuration mode.
`awplus(config)#`	
`vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#`	
`vlan 5 name ctrl-blue state enable`	Enable VLAN 5 called `ctrl-blue` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#`	
`vlan 40 name data-a state enable`	Enable VLAN 40 called `data-a` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#`	
`vlan 6 name ctrl-green state enable`	Enable VLAN 6 called `ctrl-green` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#`	
`exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Add physical port1.0.1 to these VLANs (on Transit Nodes D and E)

`awplus(config)#`	
`interface port1.0.1`	Specify the physical `interface (port1.0.1)` that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 5`	Enable VLAN 5 on this port.
`awplus(config-if)#`	
`switchport trunk native vlan none`	Remove the native VLAN.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 3: Add physical port1.0.2 to these VLANs (on Transit Nodes D and E)

`awplus(config)#`	
`interface port1.0.2`	Specify the physical `interface (port1.0.2)` that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 5`	Enable VLAN 5 (ctrl-blue) on this port.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 6`	Enable VLAN 6 (ctrl-green) on this port.
`awplus(config-if)#`	
`switchport trunk native vlan none`	Remove the native VLAN.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 4: Add physical port1.0.3 to these VLANs (on Transit Nodes D and E)

`awplus(config)#`	
`interface port1.0.3`	Specify the physical `interface (port1.0.3)` that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 6`	Enable VLAN 6 on this port.
`awplus(config-if)#`	
`switchport trunk native vlan none`	Remove the native VLAN.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 5: Create the EPSR instance called "blue" on a transit node, make VLAN 5 the control VLAN (on Transit Nodes D and E)

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr blue mode transit controlvlan 5`	Create an EPSR instance called `blue` on `vlan 5`. Make `vlan 5` the control VLAN. Make this node a transit node.

Step 6: Add a data VLAN to the EPSR instance called "blue" (on Transit Nodes D and E)

`awplus(config-epsr)#`	
`epsr blue datavlan 40`	On the EPSR instance called `blue` make `vlan 40` the data VLAN.

Step 7: Assign a priority to the ring instance (on Transit Nodes D and E)

This step is **mandatory on transit nodes that connect to a common segment**, and good practice on other transit nodes.

`awplus(config-epsr)#`	
`epsr blue priority 120`	Set the ring instance priority to 120 - the value selected for the ring.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 8: Enable the EPSR instance called "blue" (on Transit Nodes D and E)

`awplus(config-epsr)#`	
`epsr blue state enable`	Enable the EPSR instance named `blue`.

Step 9: Create the EPSR instance called "green" on a transit node, make VLAN 6 the control VLAN (on Transit Nodes D and E)

`awplus(config-epsr)#`	
`epsr green mode transit controlvlan 6`	Create an EPSR instance called `green` on `vlan 6`. Make `vlan 6` the control VLAN. Make this node a transit node.

Step 10: Add a data VLAN to the EPSR instance called "green" (on Transit Nodes D and E)

`awplus(config-epsr)#`	
`epsr green datavlan 40`	On the EPSR instance called `green` make `vlan 40` the data VLAN.

Step 11: Assign a priority to the ring instances (on Transit Nodes D and E)

This step is **mandatory on transit nodes that connect to a common segment**, and good practice on other transit nodes.

`awplus(config-epsr)#`	
`epsr green priority 60`	Set the ring instance priority to 60 - this being the priority selected for the ring.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 12: Enable the EPSR instance called "green" (on Transit Nodes D and E)

`awplus(config-epsr)#`	
`epsr green state enable`	Enable the EPSR instance named `green`.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 13: Add the physical port 1.0.1 to these VLANs (on Transit Nodes D and E)

`awplus(config)#`	
`interface port1.0.1`	Specify the physical interface (`port1.0.1`) that you are configuring, and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 14: Add the physical port1.0.2 to these VLANs (on Transit Nodes D and E)

`awplus(config)#`	
`interface port1.0.2`	Specify the physical interface (`port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 15: Add the physical port1.0.3 to these VLANs (on Transit Nodes D and E)

`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

On Ring 2 - configure the Transit Node F

Step 1: Create the control and data VLANs (on Transit Node F)

`awplus#` `configure terminal`	Enter the Global Configuration mode.
`awplus(config)#` `vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)#` `vlan 6 name ctrl-green state enable`	Enable VLAN 6 called `ctrl-green` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `vlan 40 name data-a state enable`	Enable VLAN 40 called `data-a` on the transit node. Specifying the enable state allows forwarding of frames on the VLAN-aware node.
`awplus(config-vlan)#` `exit`	Exit the VLAN Configuration mode and enter the Global Configuration mode.

Step 2: Create the EPSR instance called “green” on a transit node, make VLAN 6 the control VLAN (on Transit Node F)

`awplus(config)#` `epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#` `epsr green mode transit controlvlan 6`	Create an EPSR instance called `green` on `vlan 6`. Make `vlan 6` the control VLAN. Make this node a transit node.

Step 3: Add a data VLAN to the EPSR instance called “green” (on Transit Node F)

`awplus(config-epsr)#` `epsr green datavlan 40`	On the EPSR instance called `green` make `vlan 40` the data VLAN.

Step 4: Enable the EPSR instance called “green” (on Transit Node F)

`awplus(config-epsr)#` `epsr green state enable`	Enable the EPSR instance named `green`.

Step 5: Assign a priority to the ring instance (on Transit Node F)

This step is **mandatory on transit nodes that connect to a common segment**, and good practice on other transit nodes.

`awplus(config-epsr)#`	
`epsr green priority 120`	Set the ring instance priority to the priority selected for the ring 120.
`awplus(config-epsr)#`	
`exit`	Exit the EPSR Configuration mode.

Step 6: Add the physical port1.0.1 to VLANs 6 and 40 (on Transit Node F)

`awplus(config)#`	
`interface port1.0.1`	Specify the physical interface (`port1.0.1`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 6`	Enable VLAN 6 on this port.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#`	
`switchport trunk native vlan none`	Remove the native VLAN
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 7: Add the physical port1.0.2 to VLANs 6 and 40 (on Transit Node F)

`awplus(config)#` `interface port1.0.2`	Specify the interface (`port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#` `switchport mode trunk`	Set the switching characteristics of this port to Trunk mode.
`awplus(config-if)#` `switchport trunk allowed vlan add 6`	Enable VLAN 6 on this port.
`awplus(config-if)#` `switchport trunk allowed vlan add 40`	Enable VLAN 40 on this port.
`awplus(config-if)#` `switchport trunk native vlan none`	Remove the native VLAN
`awplus(config-if)#` `exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Sample Show Output

For the above network configuration, running the command **show epsr** on node R1 will display the following output when operating normally. Note the blocked state of its secondary port.

Figure 57-14: Output from the show epsr command run on Master Node R1 - with Ring 1 - EPSR instance blue operating normally

```
 EPSR Information
-------------------------------------------------------------------
 Name .....................blue
 Mode .....................Master
 Status ...................Enabled
 State ....................Complete
 Control Vlan .............5
 Data VLAN(s) .............40
 Interface Mode ...........Ports Only
 Primary Port .............port1.0.1
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Secondary Port ...........port1.0.2
   Status .................Blocked
   Is On Common Segment ...No
   Blocking Control .......Physical
 Hello Time ...............1 s
 Failover Time ............2 s
 Ring Flap Time ...........0 s
 Trap .....................Enabled
 Enhanced Recovery ........Disabled
 Priority .................120
-------------------------------------------------------------------
```

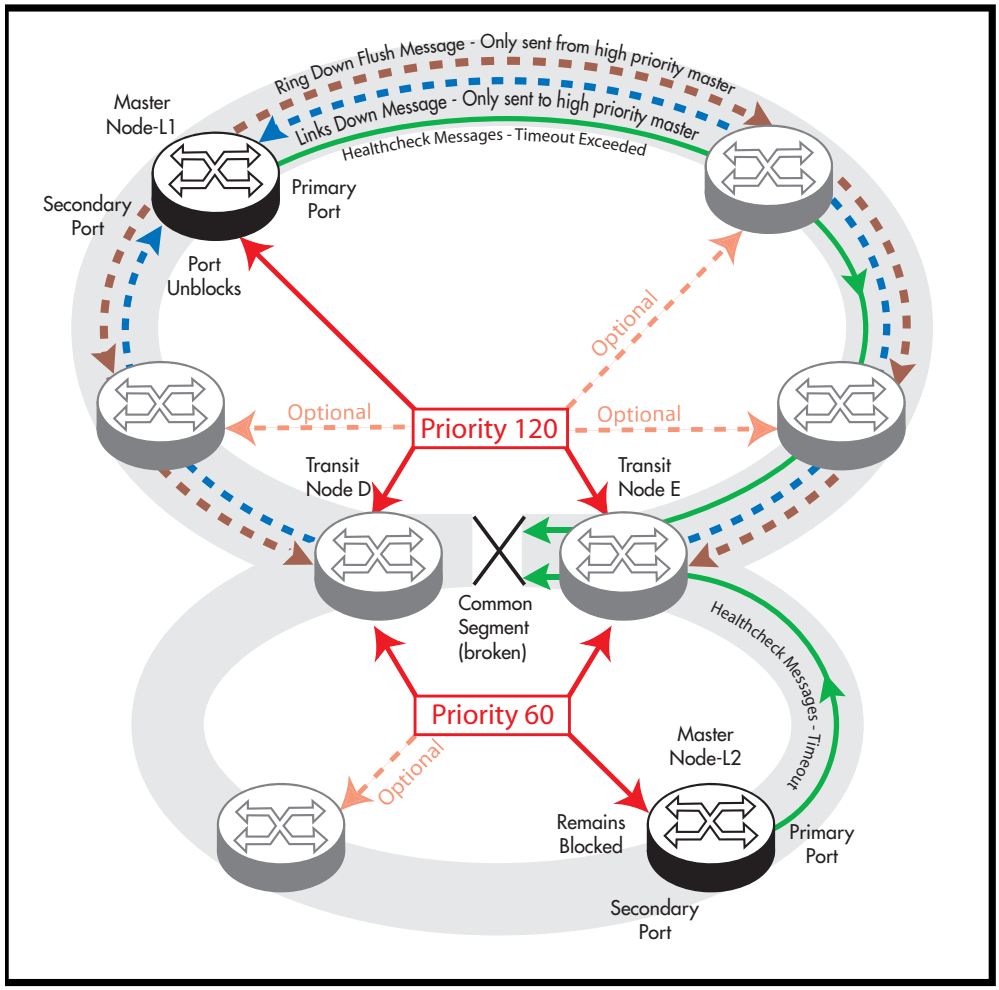
If a fault occurs somewhere within the blue network ring the Master Node-R1 would respond by placing its secondary port into the forwarding state. Figure **Figure 57-15** displays its resultant state. Note that the state of its secondary port has now moved from Blocked, Forwarding.

Figure 57-15: Output from the show epsr command run on Master Node R2, where a break exists within the Ring 1 - EPSR instance blue

```
 EPSR Information
-------------------------------------------------------------------
 Name .....................blue
 Mode .....................Master
 Status ...................Enabled
 State ....................Failed
 Control Vlan .............6
 Data VLAN(s) .............40
 Interface Mode ...........Ports Only
 Primary Port .............port1.0.1
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Secondary Port ...........port1.0.2
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Hello Time ...............1 s
 Failover Time ............2 s
 Ring Flap Time ...........0 s
 Trap .....................Enabled
 Enhanced Recovery ........Disabled
 Priority .................60
-------------------------------------------------------------------
```

If a fault occurs in the common segment of the ring then the Master Node-R2 being on the lower priority ring would detect a timeout of its transmitted Healthcheck Message. It would also detect the absence of the expected **Ring Down Flush** message, see **Figure 57-16**. The Master node then assumes that there is a break somewhere in the Common Segment, and will display the status shown in **Figure 57-17**.

Figure 57-16: EPSR behavior with a faulty common segment and superloop enabled



Note that the secondary port on Master Node-L2 remains in the blocked state; its state now appears in show output as being as blocked (for superloop prevention). See **Figure 57-17**.

The Master-L1 on the blue ring will also detect a timeout in the healthcheck message, but because ring 1 has the higher priority (of 120), it will receive a Links Down message from each of the transit nodes (D and E) that connect to the common segment. As a result, the state of the Master Node will be as shown in **Figure 57-17**; note particularly the change in its Secondary Port status.

Figure 57-17: Output from the show epsr command run on Master Node L2 (green)

```
 EPSR Information
-------------------------------------------------------------------
 Name .....................green
 Mode .....................Master
 Status ...................Enabled
 State ....................Failed
 Control Vlan .............6
 Data VLAN(s) .............40
 Interface Mode ...........Ports Only
 Primary Port .............port1.0.1
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Secondary Port ...........port1.0.2
   Status .................Blocked (for superloop prevention)
   Is On Common Segment ...No
   Blocking Control .......Physical
 Hello Time ...............1 s
 Failover Time ............2 s
 Ring Flap Time ...........0 s
 Trap .....................Enabled
 Enhanced Recovery ........Disabled
 Priority .................60
-------------------------------------------------------------------
```

Figure 57-18: Output from the show epsr command run on Master Node L1 (blue)

```
 EPSR Information
-------------------------------------------------------------------
 Name .....................blue
 Mode .....................Master
 Status ...................Enabled
 State ....................Failed
 Control Vlan .............6
 Data VLAN(s) .............40
 Interface Mode ...........Ports Only
 Primary Port .............port1.0.1
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Secondary Port ...........port1.0.2
   Status .................Forwarding
   Is On Common Segment ...No
   Blocking Control .......Physical
 Hello Time ...............1 s
 Failover Time ............2 s
 Ring Flap Time ...........0 s
 Trap .....................Enabled
 Enhanced Recovery ........Disabled
 Priority .................60
-------------------------------------------------------------------
```

Adding a New Data VLAN to a Functioning Superloop Topology

This example shows how to add another data VLAN called **data-b** to the superloop topology. We recommend that you apply the configuration steps in the order shown.

1. Add VLAN to the common segment (for both instances)
2. Add VLAN to blue master
3. Add VLAN to other blue transits
4. Add VLAN to green master
5. Add VLAN to other green transits

On Ring 1 EPSR instance blue - configure each of the transit nodes that connect to the common segment

Select one of the transit nodes that connects to the common segment, and carry out the following steps:

Step 1: Add VLAN 50 to the VLAN database and set its state to enable

`awplus#`	
`configure terminal`	Enter terminal config mode
`awplus(config)#`	
`vlan database`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`vlan 50 name data-b enable`	Create VLAN 50, name it data-b and enable it.

Step 2: Add the VLAN 50 to the EPSR Instances called “blue” and “green” on the transit nodes

`awplus(config)#`	
`epsr configuration`	Enter the EPSR Configuration mode.
`awplus(config-epsr)#`	
`epsr blue datavlan 50`	On the EPSR instance called `blue` add `vlan 50` as a data VLAN.
`awplus(config-epsr)#`	
`epsr green datavlan 50`	On the EPSR instance called `green` add `vlan 50` as a data VLAN.

Step 3: Add the common physical port (port1.0.2 in this example) to VLAN 50

`awplus(config)#`	
`interface port1.0.2`	Specify the physical interface (`port1.0.2`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 50`	Enable VLAN 50 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface mode and enter the Global Configuration mode.

Step 4: to VLAN 50

`awplus(config)#`	
`interface port1.0.1`	Specify the interface (`port1.0.1`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 50`	Enable VLAN 50 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Step 5: Add physical port1.0.3 to VLAN 50

`awplus(config)#`	
`interface port1.0.3`	Specify the interface (`port1.0.3`) that you are configuring and enter the Interface Configuration mode.
`awplus(config-if)#`	
`switchport trunk allowed vlan add 50`	Enable VLAN 50 on this port.
`awplus(config-if)#`	
`exit`	Exit the Interface Configuration mode and enter the Global Configuration mode.

Select the next transit node that connects to the common segment, and repeat the above steps:

On Ring 1 EPSR instance blue - Add VLAN 50 to the Master Node

Carry out this process using the same basic procedure shown in Steps 1 to 5

On Ring 1 EPSR instance blue - Add VLAN 50 to the transit nodes

Carry out this process using the same basic procedure shown in Steps 1 to 5

On Ring 2 EPSR instance green - Add VLAN 50 to the Master Node

Carry out this process using the same basic procedure shown in Steps 1 to 5

On Ring 2 EPSR instance green - Add VLAN 50 to the remaining transit node

Carry out this process using the same basic procedure shown in Steps 1 to 5

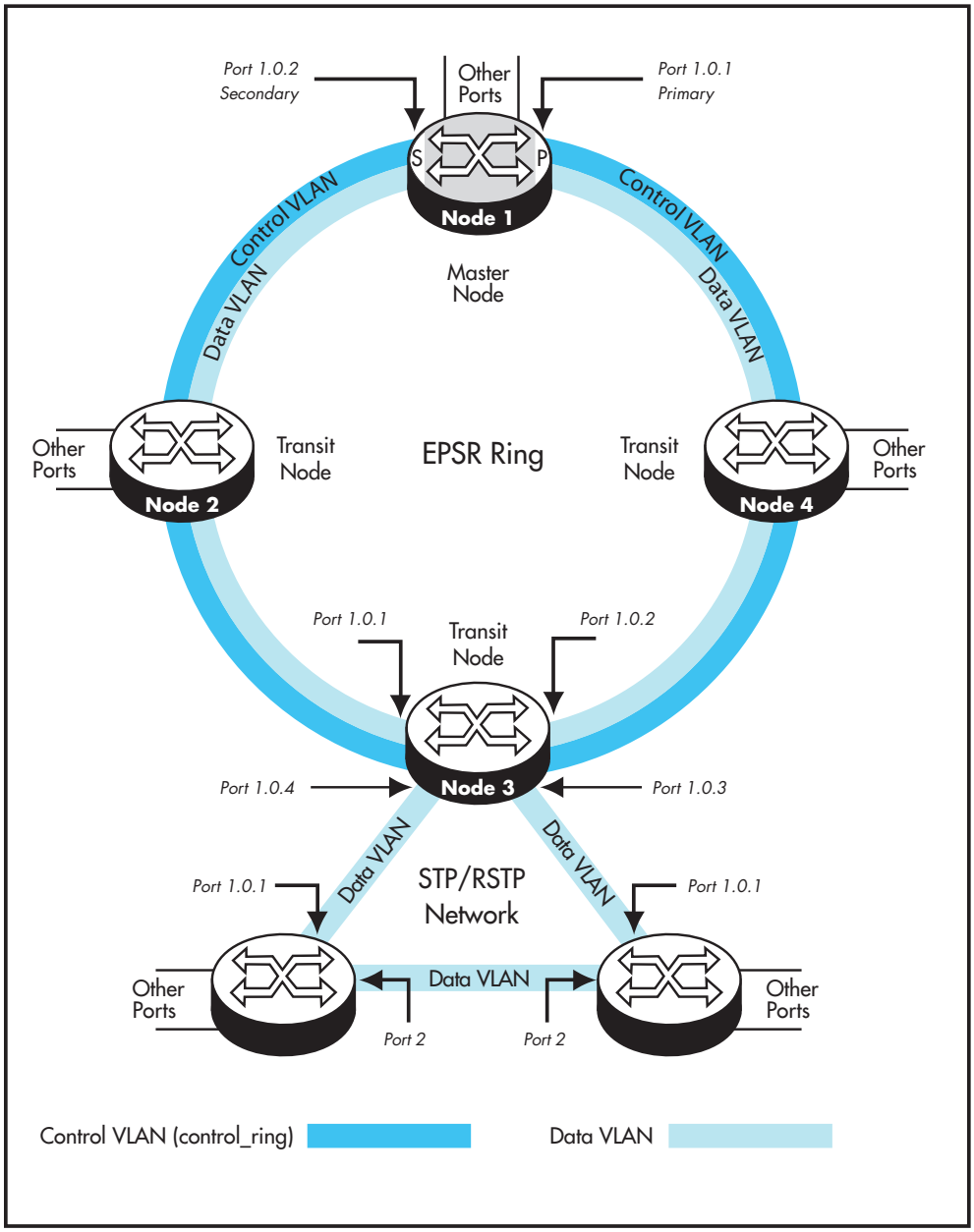
EPSR and Spanning Tree Operation

EPSR and the Spanning Tree Protocol (STP) address data loop prevention, although they do it differently. EPSR is manually configured to explicitly identify which links are broken in the defined ring, whereas STP/RSTP calculates where to break links based on user-provided values (metrics) that are compared to determine the “best” (or lowest cost) paths for data traffic.

At the practical level you can use these two techniques to create complementary hybrid EPSR /STP configurations. This configuration might have a high speed fiber loop topology backbone-controlled and managed using EPSR. Lobes could extend out from each loop node into a user mesh network. Any loops in this mesh network would be controlled and managed using STP/RSTP. Note that EPSR and STP cannot share the same ports.

The following figure shows a basic combined EPSR / STP network.

Figure 57-19: EPSR and spanning tree operation



Chapter 58: EPSR Commands

Command List 58.2
debug epsr 58.3
epsr 58.4
epsr configuration 58.5
epsr datavlan 58.6
epsr enhancedrecovery enable 58.7
epsr mode master controlvlan primary port 58.8
epsr mode transit controlvlan 58.9
epsr priority 58.10
epsr state 58.11
epsr trap 58.12
show debugging epsr 58.12
show epsr 58.13
show epsr common segments 58.16
show epsr config-check 58.17
show epsr <epsr-instance> 58.18
show epsr <epsr-instance> counters 58.18
show epsr counters 58.19
show epsr summary 58.20
undebug epsr 58.20

Command List

This chapter provides an alphabetical reference for commands used to configure EPSR. For more information, see **Chapter 57, EPSR Introduction and Configuration**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

debug epsr

This command enables EPSR debugging.

The **no** variant of this command disables EPSR debugging.

Syntax

```
debug epsr {info|msg|pkt|state|timer|all}
no debug epsr {info|msg|pkt|state|timer|all}
```

Parameter	Description
`info`	Send general EPSR information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above information from being sent to the console.
`msg`	Send the decoded received and transmitted EPSR packets to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`pkt`	Send the received and transmitted EPSR packets as raw ASCII text to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`state`	Send EPSR state transitions to the console. Using this parameter with the **no debug epsr** command will explicitly exclude state transitions from being sent to the console.
`timer`	Send EPSR timer information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude timer information from being sent to the console.
`all`	Send all EPSR debugging information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude any debugging information from being sent to the console.

Mode Privileged Exec and Global Configuration

Examples To enable state transition debugging, use the command:

```
awplus# debug epsr state
```

To disable EPSR packet debugging, use the command:

```
awplus# no debug epsr pkt
```

Related Commands undebug epsr

epsr

This command sets the timer values for an EPSR instance. These are only valid for master nodes.

Note This command will only run on switches that are capable of running as an EPSR master node. However, even if your switch cannot function as an EPSR master node; you will still need to configure this command on whatever switch is the master within your EPSR network.
Refer to the manual of your master node's switch.

Syntax

```
epsr <epsr-instance> {hellotime <1-32767>|failovertime <2-65535>
   ringflaptime <0-65535>}

no epsr <epsr-instance>
```

Caution **Using the "no" variant of this command will remove the specified EPSR instance.**

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`hellotime` *<1-32767>*	The number of seconds between the transmission of health check messages.
`failovertime` *<2-65535>*	The number of seconds that a master waits for a returning health check message before entering the failed state. **The failover time should be greater than twice the hellotime.** This is to force the master node to wait until it detects the absence of two sequential healthcheck messages before entering the failed state.
`ringflaptime` *<0-65535>*	The minimum number of seconds that a master must remain in the failed state.

Mode EPSR Configuration

Examples To set the hellotimer to 5 seconds for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue hellotime 5
```

To delete the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue
```

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
epsr configuration
epsr datavlan
epsr state
epsr trap
show epsr

epsr configuration

Use this command to enter EPSR Configuration mode so that EPSR can be configured.

Syntax `epsr configuration`

Mode Global Configuration

Example To change to EPSR mode, use the command:

```
awplus(config)# epsr configuration
```

Related Commands **epsr mode master controlvlan primary port**
epsr
show epsr

epsr datavlan

This command adds a data VLAN or a range of VLAN identifiers to a specified EPSR instance.

The **no** variant of this command removes a data vlan or data vlan range from an EPSR instance.

Syntax

```
epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
no epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`datavlan`	Adds a data VLAN to be protected by the EPSR instance.
<vlanid>	The VLAN's VID - a number between 1 and 4094 excluding the number selected for the control VLAN.
<vlanid-range>	Specify a range of VLAN identifiers using a hyphen to separate identifiers.

Mode EPSR Configuration

Usage We suggest setting the epsr controlvlan to vlan2 using the **epsr mode master controlvlan primary port** and **epsr mode transit controlvlan** commands, then setting the EPSR data VLAN between to be a value 3 and 4094 using the **epsr datavlan** command.

Examples To add `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan3
```

To add `vlan2` and `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan2-vlan3
```

To remove `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan3
```

To remove `vlan2` and `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan2-vlan3
```

Related Commands

epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr

epsr enhancedrecovery enable

This command enables EPSR's enhanced recovery mode. Enhanced recovery mode enables a ring to apply additional recovery procedures when a ring with more than one break, partially mends. For more information see **"Managing Rings with Two Breaks" on page 57.6**.

The **no** variant of this command disables the enhancedrecovery mode.

Syntax

```
epsr <epsr-instance> enhancedrecovery enable
no epsr <epsr-instance> enhancedrecovery enable
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Default Default is enhancedrecovery mode disabled.

Mode EPSR Configuration

Example To apply enhanced recovery on the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue enhancedrecovery enable
```

Related Commands **show epsr**

epsr mode master controlvlan primary port

This command creates a master EPSR instance. Your switch is unable to run this command because it cannot function as an EPSR master node. To include these switches in an EPSR ring you will need to use an alternative Allied Telesis switch, such as an x610 Series switch, as the master node. For more information on this command, refer to the manual of your master EPSR node's switch.

Syntax

```
epsr <epsr-instance> mode master controlvlan <2-4094> primaryport
   <port>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`mode`	Determines the node is acting as a master.
`master`	Sets switch to be the master node for the named EPSR ring.
`controlvlan`	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.
`primaryport`	Primary port for the EPSR instance.
<port>	The primary port. The port may be a switch port (e.g. `port1.0.4`) or a static channel group (e.g. `sa2`). It cannot be a dynamic (LACP) channel group.

Mode EPSR Configuration

Example To create a master EPSR instance called `blue` with `vlan2` as the control VLAN and `port1.0.1` as the primary port, use the command:

```
awplus(config-epsr)# epsr blue mode master controlvlan vlan2
                     primaryport port1.0.1
```

Related Commands

epsr mode transit controlvlan
show epsr

epsr mode transit controlvlan

This command creates a transit EPSR instance.

Syntax `epsr <epsr-instance> mode transit controlvlan <2-4094>`

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`mode`	Determines the node is acting as a transit node.
`transit`	Sets switch to be the transit node for the named EPSR ring.
`controlvlan`	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.

Note

The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch or stacked node. However, we advise against this because in certain situations it can produce unpredictable results.

If the control VLAN contains more than two ports (or static channels) an algorithm selects the two ports or channels with the lowest number to be the ring ports. However if the switch has only one channel group is defined to the control vlan, EPSR will not operate on the secondary port.

EPSR does not support Dynamic link aggregation (LACP).

Mode EPSR Configuration

Example To create a transit EPSR instance called `blue` with `vlan2` as the control VLAN, use the command:

```
awplus(config-epsr)# epsr blue mode transit controlvlan vlan2
```

Related Commands

epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr

epsr priority

This command sets the priority of an EPSR instance on an EPSR node. Priority is used to prevent "superloops" forming under fault conditions with particular ring configurations. Setting a node to have a priority greater than one, also has the effect of turning on **superloop protection**.

The **no** variant of this command returns the priority of the EPSR instance back to its default value of 0, which also disables EPSR Superloop prevention.

Syntax

```
epsr <epsr-instance> priority <0-127>

no <epsr-instance> priority
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`priority`	The priority of the ring instance selected by the epsr-name parameter.
<0-127>	The priority to be applied (0 is the lowest priority and represents no superloop protection).

Default The default priority of an EPSR instance on an EPSR node is 0. The negated form of this command resets the priority of an EPSR instance on an EPSR node to the default value.

Mode EPSR Configuration

Example To set the priority of the EPSR instance called `blue` to the highest priority (127), use the command:

```
awplus(config-epsr)# epsr blue priority 127
```

To reset the priority of the EPSR instance called `blue` to the default (0), use the command:

```
awplus(config-epsr)# no epsr blue priority
```

Related Commands **epsr configuration**

epsr state

This command enables or disables an EPSR instance.

Syntax `epsr <epsr-instance> state {enabled|disabled}`

Parameter	Description
<epsr-instance>	The name of the EPSR instance.
`state`	The operational state of the ring.
`enabled`	EPSR instance is enabled.
`disabled`	EPSR instance is disabled.

Mode EPSR Configuration

Example To enable the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue state enabled
```

Related Commands **epsr mode master controlvlan primary port**
epsr mode transit controlvlan

epsr trap

This command enables SNMP traps for an EPSR instance. The traps will be sent when the EPSR instance changes state.

The **no** variant of this command disables SNMP traps for an EPSR instance. The traps will no longer be sent when the EPSR instance changes state.

Syntax

```
epsr <epsr-instance> trap
no epsr <epsr-instance> trap
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`trap`	SNMP trap for the EPSR instance.

Mode EPSR Configuration

Example To enable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue trap
```

To disable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue trap
```

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr

show debugging epsr

This command shows the debugging modes enabled for EPSR.

Syntax

```
show debugging epsr
```

Mode User Exec and Privileged Exec

Example To show the enabled debugging modes, use the command:

```
awplus# show debugging epsr
```

Related Commands
debug epsr

show epsr

This command displays information about all EPSR instances.

Syntax `show epsr`

Mode User Exec and Privileged Exec

Example To show the current settings of all EPSR instances, use the command:

```
awplus# show epsr
```

Output The following examples show the output display for a **non** superloop topology network.

Figure 58-1: Example output from the show epsr command run on a transit node

```
EPSR Information
------------------------------------------------------------------
 Name ........................... test2
 Mode ........................... Transit
 Status ......................... Enabled
 State .......................... Links-Up
 Control Vlan ................... 2
 Data VLAN(s) ................... 10
 Interface Mode ................. Ports Only
 First Port ..................... port1.0.1
 First Port Status .............. Down
 First Port Direction .......... Unknown
 Second Port .................... port1.0.2
 Second Port Status ............. Down
 Second Port Direction ......... Unknown
 Trap ........................... Enabled
 Master Node .................... Unknown
 Enhanced Recovery .............. Disabled
------------------------------------------------------------------
```

The following example shows the output display for superloop topology network.

Figure 58-2: Example output from the show epsr command run on a Transit Node

```
 EPSR Information
----------------------------------------------------------------
 Name ......................... test4
 Mode ......................... Transit
 Status ....................... Enabled
 State ........................ Complete
 Control Vlan ................. 4
 Data VLAN(s) ................. 20
 Interface Mode ............... Ports Only
 Primary Port ................. port1.0.3
   Status ..................... Forwarding (logically blocking)
   Is On Common Segment ....... No
   Blocking Control ........... Physical
 Secondary Port ............... port1.0.4
   Status ..................... Blocked
   Is On Common Segment ....... No
   Blocking Control ........... Physical
 Hello Time ................... 1 s
 Failover Time ................ 2 s
 Ring Flap Time ............... 0 s
 Trap ......................... Enabled
 Enhanced Recovery ............ Disabled
 SLP Priority ................. 12
----------------------------------------------------------------
```

Table 58-1: Parameters displayed in the output of the show epsr command

Parameter on Master Node	Parameter on Transit Node	Description
Name	Name	The name of the EPSR instance.
Mode	Mode	The mode in which the EPSR instance is configured - either Master or Transit
Status	Status	Indicates whether the EPSR instance is enabled or disabled
State	State	Indicates state of the EPSR instance's state machine. Master states are: Idle, Complete, and Failed. Transit states are Links-Up, Links-Down, and Pre-Forwarding.
Control Vlan	Control Vlan	Displays the VID of the EPSR instance's control VLAN.
Data VLAN(s)	Data VLAN(s)	The VID(s) of the instance's data VLANs.
Interface Mode	Interface Mode	Whether the EPSR instance's ring ports are both physical ports (Ports Only) or are both static aggregators (Channel Groups Only).
Primary Port	First Port	The EPSR instance's primary ring port.
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port because it does not have physical control of it.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment.

Table 58-1: Parameters displayed in the output of the show epsr command (cont.)

Parameter on Master	Parameter on Transit	Description(cont.)
- Blocking Control	- Blocking Control	Whether the instance has “physical” or “logical” control of the ring port's blocking in the instance's data VLANs.
Secondary Port	Second Port	The EPSR instance's secondary port.
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, “(logical)” indicates the instance has only logically set the blocking state of the port, because it does not have physical control of it. Note that on a master configured for SuperLoop Prevention (non-zero priority) its secondary ring port can be physically forwarding, but logically blocking. This situation arises when it is not the highest priority node in the topology (and so does not receive LINKS-DOWN messages upon common segment breaks) and a break on a common segment in its ring is preventing reception of its own health messages.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by “Upstream”. The other ring port is then “Downstream”
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, “(highest rank)” indicates it is the highest priority instance on that common segment
- Blocking Control	- Blocking Control	Whether the instance has “physical” or “logical” control of the ring port's blocking in the instance's data VLANs
Hello Time		The EPSR instance's setting for the interval between transmissions of health check messages (in seconds)
Failover Time		The time (in seconds) the EPSR instance waits to receive a health check message before it decides the ring is down
Ring Flap Time		The minimum time the EPSR instance must remain in the failed state
Trap	Trap	Whether the EPSR instance has EPSR SNMP traps enabled
Enhanced Recovery	Enhanced Recovery	Whether the EPSR instance has enhanced recovery mode enabled
SLP Priority	SLP Priority	The EPSR instance's priority (for SuperLoop Prevention)

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr counters

show epsr common segments

This command displays information about all the superloop common segment ports on the switch

Syntax `show epsr common segments`

Example To display information about all the superloop common segment ports on the switch, use the command:

```
awplus# show epsr common segments
```

Figure 58-3: Example output from the show epsr common segments command

```
EPSR Common Segments

Common Seg  EPSR                          Port    Phys Ctrl  Ring
Ring Port   Instance        Mode     Prio  Type    of Port?   Port Status
-------------------------------------------------------------------------------
port1.0.24  test_inst_Red   Transit  127   Second    Yes      Fwding
            test_inst_Blue  Transit  126   Second    No       Fwding (logical)
            test_inst_Green Transit  125   First     No       Fwding (logical)

sa4         testA           Master    15   Primary   Yes      Blocking
            testB           Transit   14   Second    No       Fwding (logical)

sa5         test_55         Transit    8   First     Yes      Down
            test_77         Transit    7   First     No       Down
-------------------------------------------------------------------------------
```

Related Commands
- show epsr
- show epsr summary
- show epsr counters

show epsr config-check

This command checks the configuration of a specified EPSR instance, or all EPSR instances.

If an instance is enabled, this command will check for the following errors or warnings:

- The control VLAN has the wrong number of ports.
- There are no data VLANs.
- Some of the data VLANs are not assigned to the ring ports.
- The failover time is less than 5 seconds, for a stacked device.
- The instance is a master that shares a common segment with a higher priority instance.
- The instance is a master that shares a common segment with another master.
- The instance is a master with its secondary port on a common segment.

Syntax `show epsr [<instance>] config-check`

Parameter	Description
<instance>	Name of the EPSR instance to check on.

Mode User Exec and Privileged Exec

Example To check the configuration of all EPSR instances and display the results, use the command:

```
awplus# show epsr config-check
```

Figure 58-4: Example output from the show epsr config-check command

```
EPSR             Status   Description
Instance
------------------------------------------------------------------------------
red              Warning  Failover time is 2s but should be 5s because device.
                            is stacked
white            OK.
blue             Warning  Primary port is not in data VLANs 29-99.
orange           OK.

Don't forget to check that this node's configuration is consistant with all
other nodes in the ring.
------------------------------------------------------------------------------
```

Related Commands show epsr

show epsr <epsr-instance>

This command displays information about the specified EPSR instance.

Syntax `show epsr <epsr-instance>`

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the current settings of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue
```

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr counters

show epsr <epsr-instance> counters

This command displays counter information about the specified EPSR instance.

Syntax `show epsr <epsr-instance> counters`

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the counters of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue counters
```

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr

show epsr counters

This command displays counter information about all EPSR instances.

Syntax `show epsr counters`

Mode User Exec and Privileged Exec

Example To show the counters of all EPSR instances, use the command:

```
awplus# show epsr counters
```

Related Commands
epsr mode master controlvlan primary port
epsr mode transit controlvlan
show epsr

show epsr summary

This command displays summary information about all EPSR instances on the switch

Syntax `show epsr summary`

Mode User Exec and Privileged Exec

Example To display epsr summary information, use the command:

```
awplus# show epsr summary
```

Example To display EPSR summary information, use the command:

```
awplus# show epsr summary
```

Figure 58-5: Example output from the show epsr summary command

```
EPSR Summary Information

Abbreviations:
  M = Master node
  T = Transit node
  C = is on a common segment with other instances
  P = instance on a common segment has physical control of the shared port's
        data VLAN blocking
  LB = ring port is Logically Blocking - applicable to master only

EPSR                                  Ctrl       Primary/1st     Secondary/2nd
Instance      Mode Status   State     VLAN  Prio Port Status     Port Status
-------------------------------------------------------------------------------
test-12345      T  Enabled  Links-Down    6  127  Blocking (C,P)  Blocking (C,P)
test1           M  Enabled  Complete      5   12  Fwding          Fwding (LB)
test2           T  Enabled  Pre-Fwding    4  126  Fwding (C)      Blocking (C)
localB          T  Disabled Idle         40    0  Unknown         Unknown
localC          T  Disabled Idle         41    0  Unknown         Unknown
-------------------------------------------------------------------------------
```

undebug epsr

This command applies the functionality of the **no debug epsr** command on page 58.3.

Chapter 59: RRP Snooping Introduction and Commands

RRP Snooping Introduction 59.2
Command List 59.3
ip rrp snooping 59.3
show ip rrp snooping 59.4

RRP Snooping Introduction

This chapter describes the Router Redundancy Protocol (RRP) Snooping feature provided by the switch. For detailed RRP command descriptions, examples and output, see **"Command List" on page 59.3**.

The Router Redundancy Protocol (RRP) allows multiple routers to share the same virtual IP address and MAC address. In network topologies where redundant router paths or links exist, the protocol enables routers, through an election process, to designate one as the master router. This router functions as the provider of the primary path between LAN segments. Backup routers function as backup paths in the event that the master router or primary path fails.

Because the master and backup routers are able to share the same virtual IP address and MAC address, a change in data paths need not necessitate an adjustment to the default gateways on the network nodes that employ the routers. When a backup router transitions to master, it uses the same IP address as the previous master router, making the transition transparent to the network end nodes. In large networks, these transparent transitions can save the time and effort of having to manually reconfigure default gateway addresses on large numbers of network nodes when a router pathway fails.

RRP snooping on the switch facilitates the transition to a new master router by minimizing the loss of traffic, and so reduces the impact the transition could have on your network traffic.

RRP snooping monitors ingress RRP packets, determined by their source MAC address. The switch looks for packets with a source MAC address of 00:E0:2B:00:00:80-9F (ESRP).

A port receiving an RRP packet is deemed by the switch as the master RRP port. The virtual MAC address of the router is entered as a dynamic address on the port. If the switch starts to receive RRP packets on another port, it assumes that a backup router has made the transition to the role of the new master router.

The switch responds by deleting all dynamic MAC addresses from the MAC address table. As the switch relearns the addresses, the virtual MAC address of the new master router is learned on the new master RRP port, rather than the old port. Any packets received by the switch and destined for the router are forwarded to the new master router.

You cannot use RRP Snooping at the same time as the following features:

- STP, RSTP, or MSTP, except for edge ports. RSTP is enabled by default. To disable it, use the command **"no spanning-tree {mstp|rstp|stp} enable" on page 19.40**.
- Port security (the command **switchport port-security**)
- Port authentication
- EPSR
- Port mirroring

Commands Used

ip rrp snooping
show ip rrp snooping

Command List

This section provides an alphabetical reference for commands used to configure the Router Redundancy Protocol (RRP).

ip rrp snooping

Use this command to enable RRP snooping.

Use the **no** variant of this command to disable RRP Snooping.

Syntax

```
ip rrp snooping
no ip rrp snooping
```

Default The default is **disabled**.

Mode Global Configuration

Usage Use this command to enable the RRP Snooping feature. You cannot use RRP Snooping at the same time as the following features:

- STP, RSTP, or MSTP, except for edge ports. RSTP is enabled by default. To disable it, use the command **"no spanning-tree {mstp|rstp|stp} enable" on page 19.40**.
- Port security (the command **switchport port-security**)
- Port authentication
- EPSR
- Port mirroring

Examples The example below shows you how to enable RRP Snooping.

```
awplus# configure terminal
awplus(config)# ip rrp snooping
```

Related Commands **show ip rrp snooping**

show ip rrp snooping

Use this command to display Router Redundancy Protocol snooping global settings and status.

Syntax `show ip rrp snooping`

Mode Privileged Exec

Output The following example show the output display for the **show ip rrp snooping** command

```
awplus#show ip rrp snooping
Status          : Enabled

Vlan         Master     Virtual MAC Address     UpTime
------------ ---------- ----------------------- ----------------
vlan1        Port1.0.1  00e0.2b00.0085          00:00:39
-----------------------------------------------------------------
```

The following table shows the output display for the **show ip rrp snooping** command

Parameter	Description
`Status`	Displays if RRP Snooping is enabled or disabled
`Vlan`	Displays the VLAN ID
`Master`	Displays the port ID connected to the master router or the network of the master router
`Virtual MAC Address`	Displays the virtual MAC address of the router
`UpTime`	Displays the time that the current master router has been the master router

Related Commands ip rrp snooping

Part 7: Network Management

- Chapter 60 AMF Introduction and Configuration
- Chapter 61 AMF Commands
- Chapter 62 NTP Introduction and Configuration
- Chapter 63 NTP Commands
- Chapter 64 Dynamic Host Configuration Protocol (DHCP) Introduction
- Chapter 65 Dynamic Host Configuration Protocol (DHCP) Commands
- Chapter 66 SNMP Introduction
- Chapter 67 SNMP Commands
- Chapter 68 SNMP MIBs
- Chapter 69 LLDP, LLDP-MED and Voice VLAN Introduction and Configuration
- Chapter 70 LLDP Commands
- Chapter 71 SMTP Commands
- Chapter 72 RMON Introduction and Configuration
- Chapter 73 RMON Commands
- Chapter 74 Triggers Introduction
- Chapter 75 Triggers Configuration
- Chapter 76 Trigger Commands
- Chapter 77 Cable Fault Locator Introduction
- Chapter 78 Cable Fault Locator Commands

- Chapter 79 Ping Polling Introduction and Configuration
- Chapter 80 Ping-Polling Commands

Chapter 60: AMF Introduction and Configuration

Introduction to AMF 60.2
AMF on GS900MX/MPX Series Switches: AMF Edge 60.2
AMF Supported Products and Software Versions 60.2
Key Benefits of AMF 60.4
- Unified Command-Line 60.4
- Configuration Backup and Recovery 60.4
- Rolling-Reboot Upgrade 60.4
- Node Provisioning 60.5

AMF Terminology and Introduction 60.6
- AMF Network 60.6
- AMF Nodes 60.6
- Node Licensing 60.6
- Node Interconnection 60.7
- AMF Domains 60.7

AMF Network Operational Concepts 60.9
- Retention and Use of the 'Manager' Username 60.9
- Working-Set 60.9
- AMF Restricted Login 60.10
- Loop-Free Data Plane 60.10
- Aggregators 60.10
- VCStacks 60.10
- AMF External Removable Media 60.10
- AMF Interaction with QoS and ACLs 60.11
- NTP and AMF 60.11

Configuring AMF 60.13
Verifying the AMF Network 60.19
Configuring Multiple Nodes at the Same Time: the Unified CLI 60.21
- Working-Set Groups 60.22
- Executing Commands on Working-Sets 60.23
- Interactive Commands 60.26

AMF Backups 60.27
- Using External Media Storage 60.27
- Performing a Manual Backup 60.28
- Backing up to Remote Servers 60.29

Node Recovery 60.31
- Automatic Node Recovery 60.31
- Restoring a Node to a "Clean" State 60.32
- Manual Node Recovery 60.33
- Node Recovery on VCStacks 60.34

AMF Safe Configuration 60.35
- Detecting AMF Safe Configuration Operation 60.35
- AMF Safe Configuration Procedures 60.35
- Undoing an AMF Safe Configuration 60.36

Rolling-Reboot Firmware Upgrade 60.38
- Performing a Rolling-Reboot Upgrade 60.40

Node Provisioning 60.42

Introduction to AMF

The Allied Telesis Management Framework (AMF) is a suite of features that combine to simplify network management across all supported network switches from the core to the edge.

AMF also provides simplified switch recovery and firmware upgrade management. The primary function of AMF is to reduce the management and maintenance overhead on a network, while improving on responsiveness and handling of switch failures within the network.

This chapter provides a conceptual introduction to AMF together with its benefits, together with configuration guidelines showing how to use AMF in practical networks. For more information on the commands used in this chapter, see **"AMF Commands" on page 61.1**.

AMF on GS900MX/MPX Series Switches: AMF Edge

The GS900MX/MPX Series are edge switches, and can only join the edge of an AMF network.

GS900MX/MPX switches cannot act as AMF master nodes.

Each GS900MX/MPX switch can only have a single link to the rest of the AMF network, which must be an uplink to a switch that is closer to the AMF master. They cannot act as intermediate nodes, and they cannot link to other nodes at the same level of the heirarchy as themselves.

This functionality is known as "AMF Edge".

AMF Supported Products and Software Versions

The following list shows which Allied Telesis switches are capable of running AMF and indicates those capable of operating as Master Nodes.

An AMF-Master feature license is required for each AMF master node in the AMF network.

Table 60-1: AMF Nodal Capability by Switch Type

Switch Type	AMF Nodal Capability
SwitchBlade™ x8100	master or member
SwitchBlade™ x908	master or member
x930 series switches	master or member
x900 series switches	member only
x610 series switches	member only

Switch Type	AMF Nodal Capability
x510 series switches	member only
IX5-28GPX switches	member only
x310 series switches	member only
x230 series switches	member only
x210 series switches	member only
DC2552XS/L3 switches	member only
GS900MX/MPX switches	AMF edge member only

Key Benefits of AMF

The key benefits of AMF include its unified command-line, simple configuration backup and recovery process, and time-saving rolling firmware upgrade.

Unified Command-Line

The conventional means of configuring and controlling AlliedWare Plus (AW+) switches is to use their text-based command-line interface (CLI). In existing networks, the CLI is available via a serial console port and also to remote login sessions such as SSH.

AMF extends this capability from managing either a single switch to managing a whole network by using a single (unified) CLI session. Using the unified CLI, a network administrator can nominate all nodes or a subset of nodes within the AMF network to comprise an entity known as a "**working-set**". Commands can then be executed concurrently across all switching nodes within the defined working-set as if they were a single unit. Any existing configuration or diagnostic actions can thus be applied to multiple devices using a single command sequence, thus reducing maintenance costs and configuration complexity, while still retaining complete flexibility in network design and control.

Multiple AMF networks can exist side by side across a single physical network. Note that AMF treats a Virtual Chassis Stack (VCStack) as a single node.

Configuration Backup and Recovery

The **master** nodes use external storage to automatically backup the complete configuration information for all their member nodes, including boot configuration, firmware, licenses, and user scripts.

If an AMF member node should fail, the AMF process will automatically recognize and reconfigure an unconfigured replacement (standby) unit, completely recreating the stored configuration of the failed unit into the replacement unit. The new unit will then reboot and resume service, without any need for user intervention beyond physical hardware replacement and cable connection. In this way AMF provides a complete zero-touch recovery solution. For more information, see **"AMF Backups" on page 60.27**.

Rolling-Reboot Upgrade

Installing Firmware upgrades on a production network is typically an infrequent but sensitive and labor-intensive process. AMF is able to roll-out upgrades to a user-selected subset of nodes. All that needs to be entered is the target group of nodes, and the location where the new firmware is stored; AMF will then take care of the rest. Nodes are upgraded in a serial fashion, with each node tested before continuing the upgrade on the next node.

If an upgrade fails on a particular node, the upgrade process is automatically terminated and that node will revert to its previous firmware version. In this way firmware updates are almost completely hands-free, whilst also providing confidence that a bad update will not result in loss of service. For more information, see **"Performing a Rolling-Reboot Upgrade" on page 60.40**.

Node Provisioning

It is generally undesirable to have unconfigured devices connected to the network. Node provisioning enables you to preconfigure a port ready to accept and automatically configure a “clean” (as new) device for connection at a later date. This is achieved by storing the future node's configuration in the master node's backup files ready to be loaded to the new device when connected.

AMF Terminology and Introduction

This section contains a glossary of terminology used to describe AMF networking.

AMF Network

Conceptually an AMF network is a collection of interconnected network switch nodes. This interconnection in turn comprises a hierarchy of network domains. These terms are explained in more detail later in this chapter.

Network name Because networks are able to interconnect, an AMF network *name* is necessary to identify the AMF network to which any given node belongs. It follows therefore, that all nodes within a single AMF network must be configured with the same AMF network name.

AMF Nodes

Two types of nodes exist within an AMF network, Master Nodes and Member Nodes. Either type can comprise either a single switch, or a VCStack.

Master Nodes Master nodes are user defined by configuration. They then form the core domain of the AMF network. Aspects of master node functionality include:

- performing file system backups of all nodes in the AMF network.
- providing an essential component for the formation of an AMF network. That is, an AMF network cannot exist without the existence of at least one master node.
- at least one master node must be present for an AMF network to exist.

When more than one AMF master node exists in an AMF network, their operation is completely independent and unsynchronized.

Member Nodes AMF member nodes are referred to simply as nodes.

Node Licensing

Master node License AMF master nodes are supported on selected switch platforms: an AMF license is required for each master. For a list of node capability against specific switch types, see **Table 60-1 on page 60.2**

A VCStack needs to have consistent licensing on all stack members. If an AT-SBx8100 with dual CFCs is configured as an AMF master a license is only required on the CFC master, as the license with be synchronized across CFCs. If an AT-SBx908 or AT-x930 Series switch is configured as an AMF master, a license is required to be installed on **all** stack members.

When more than one AMF master node exists in an AMF network, it is important to know that these operate completely independently of each other, and there is no synchronization between AMF master nodes.

For redundancy, an AMF network can have multiple master nodes, each acting as a master for the network. However, there is no synchronization of status or data files between the masters. The behavior of a master node is not changed at all by the presence of other master nodes.

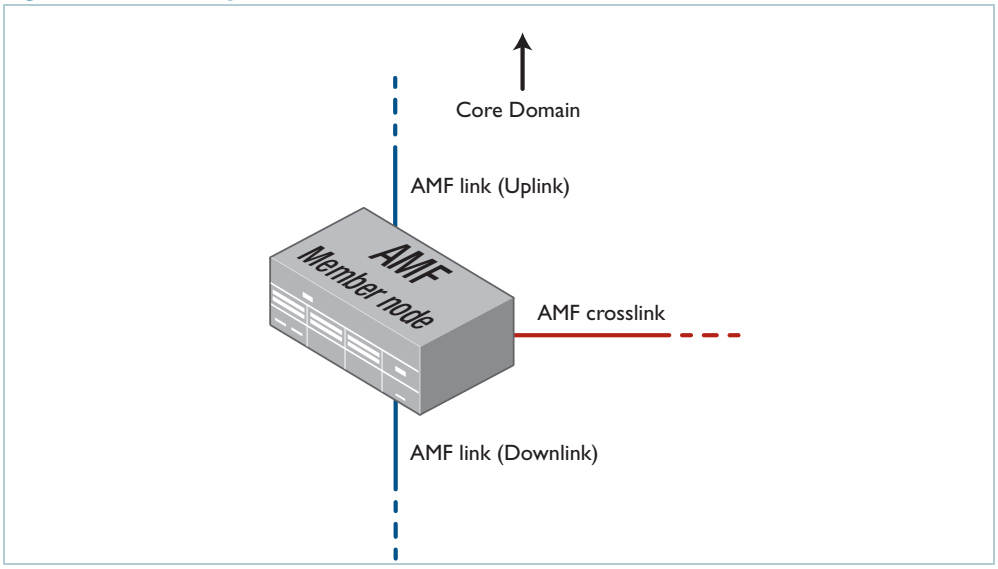
Core distance This is the distance (hop count) between a particular domain and its Core domain. The Core domain has a Core distance of 0, and the maximum recommended Core distance in an AMF network is 8.

Node Interconnection

In general, AMF nodes can connect either horizontally using crosslinks, or vertically using Uplinks/Downlinks. However, GS900MX/MPX Series switches only support uplinks, because they are edge switches, and can only join the edge of an AMF network.

The different link types are shown in the illustration below:

Figure 60-1: AMF Uplinks, Downlinks, and Crosslinks



AMF links, of either type, are used to pass AMF management traffic between nodes; however, they can also carry other network traffic. Configuring an interface as an **AMF-link** will automatically put the port into trunk mode. An AMF link can be either a single link or a static aggregator. For more information on trunk mode see **"Configuring VLANs" on page 16.3**.

Crosslinks

AMF crosslinks are used to connect AMF nodes to other AMF nodes within what is termed an AMF Domain. Configuring an interface as an AMF-crosslink will automatically put its port into trunk mode. A crosslink can be either a single link or a static aggregator.

AMF master nodes must be connected using AMF crosslinks to ensure they are part of the uppermost domain level.

Up/Down Links

Uplinks/Downlinks interconnect domains in what is a vertical hierarchy, the highest domain being the core domain.

AMF Domains

Every AMF node belongs to an AMF domain. Domains can comprise of a single node or multiple nodes. AMF master nodes are included in highest domain level, sometimes called the core domain, and all other domains are rooted in this domain.

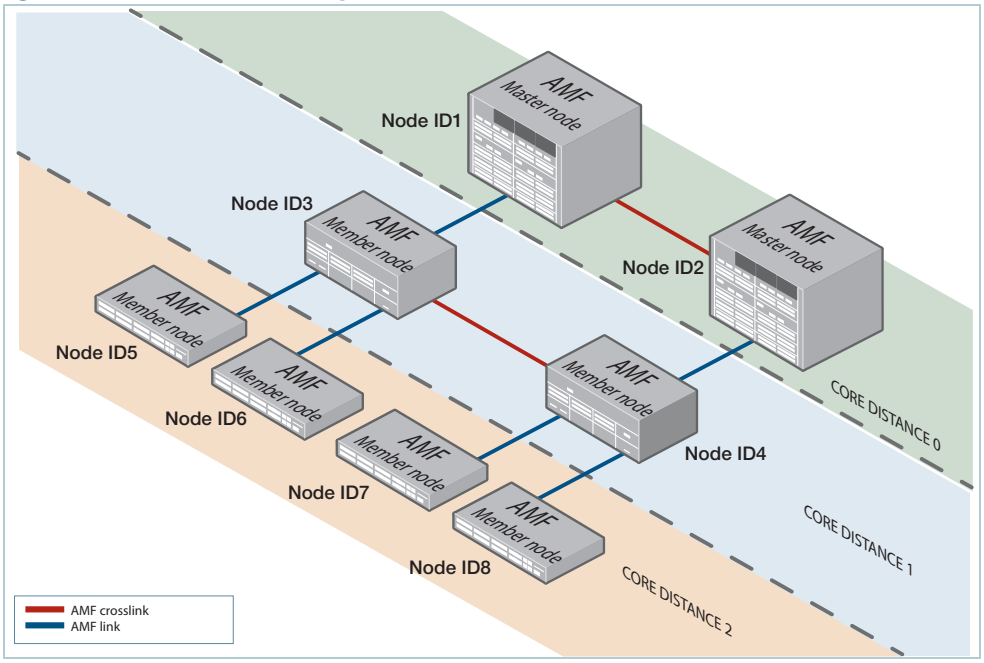
As previously mentioned, AMF domains are determined by AMF crosslinks, (see **"Working-Set" on page 60.9**). All nodes connected via AMF crosslinks form part of the same domain, and nodes connected via regular AMF links will be part of either higher of lower level domains.

Nodes within a domain must be connected in either a chain or ring topology. This means that a maximum of two crosslinks should be configured on any single node. The advantage of an AMF domain is that two links from a domain to a single higher level domain will provide redundant AMF links. We recommend that an AMF domain should only be connected to a single higher level domain, though it may be connected to multiple lower level domains. We also recommend that you set a maximum number of 12 nodes per domain.

Hop-Count

The vertical distance of a domain from the core domain is known as its Hop-Count. The illustration**"Core distance hop-counts between domains" on page 60.8** shows the relationship between nodes, domains and core distance (hop-count).

Figure 60-2: Core distance hop-counts between domains



Node provisioning

Node provisioning enables you to configure a node before it is physically present in the AMF network. When the node is eventually connected to an expectant port, it will automatically set itself up with the previously stored configuration files and release.

AMF Network Operational Concepts

Retention and Use of the 'Manager' Username

The default **username** for an AlliedWare Plus login is "manager", with a documented default **password**. Users should change this password on all their nodes to provide login security.

It is possible to add new usernames and passwords to nodes, but to retain the ability to centrally manage the network, usernames should be uniformly configured across all AMF nodes within the AMF network.

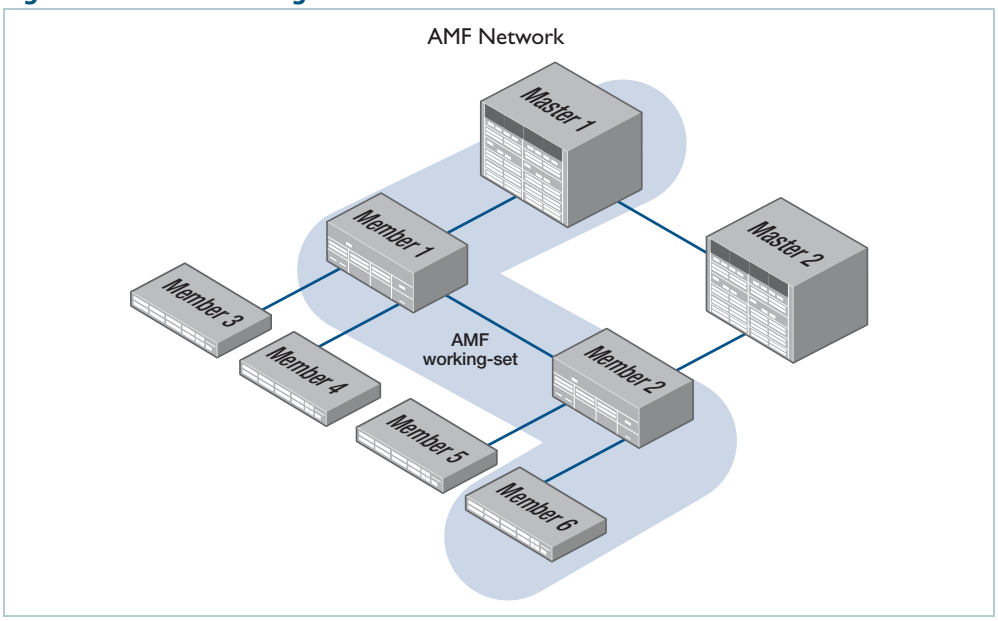
Note that managing a network with AMF is incompatible with user authentication via RADIUS or TACACS+. Use the normal local database for user authentication.

Working-Set

Conceptually a working set is a collection of switches that can then be configured centrally as if there were a single device. A working set may comprise a pre-defined group that has been automatically created based on some common set of physical attributes such as switch type etc, or it may be created by a network user for ease of configuration.

Specifying or selecting a working-set allows CLI commands to be executed on all nodes within the selected working-set with a single command. A working-set can be defined, selected and configured from any node within an AMF network. The illustration**"AMF working-set" on page 60.9** shows a number of switches which comprise a working set.

Figure 60-3: AMF working-set



AMF Restricted Login

By default, a user logged into any node on an AMF network is able to manage any other node by using either working-sets or AMF remote login (provided the login username exists on all nodes). Where the access provided by this feature is too wide, or contravenes network security restrictions, this access can be limited by running the command **"atmf restricted-login" on page 61.47**. This command will not be saved in the running configuration; it is a network property that can be enabled or disabled from any AMF master. The status of restricted-login will be retained over a reboot.

When restricted login is enable on the network, only the AMF Master nodes are able to create working-sets or manage other devices via AMF remote-logins. Other nodes may remote login to the AMF Master, but they will require password authentication on that master, and will then be able to create working-sets originating from the Master.

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Loop-Free Data Plane

The current version of AMF does not control the data plane, so it is a requirement that the network is configured such that the data plane (i.e. the paths defined by the data VLANs) is kept loop free.

Aggregators

Dynamic Aggregators (LACP) cannot be used on ports configured as AMF links or cross-links. Therefore any aggregated links in an AMF network need to be configured as static aggregators.

VCStacks

If any VCStacks are included as AMF nodes it is a requirement that the *VCS virtual MAC* feature is enabled to ensure correct operation of the AMF network. If the VCStack is running as an AMF master node and backup is required, then removable external storage media should be installed in both stack members.

AMF External Removable Media

In order to maintain a recovery capability, all AMF master nodes require external storage media installed, such as a USB or SD card. This external storage is used to hold a backup of all relevant files from all nodes within the AMF network, including other master nodes, so it must be large enough to accommodate all of the backed up files. Files that are backed up include all configuration files, release files, and scripts, but do not include files like core dumps, exception logs, or technical support files.

Typically a *4GB* capacity external media device would be of sufficient size to hold backups for a *40 node* AMF network.

AMF Interaction with QoS and ACLs

It's important that ACL and QoS rules do not block any traffic on VLANs 4091 and 4092 because they are the default AMF control VLANs. Similarly, ACL and QoS rules should not block any Layer 3 traffic on 172.31.0.* or 172.31.128.* these being the default AMF management traffic subnets. Packets with protocol type 0xfbae and BPDU packets that use the MAC address: 0180.c200.002e should also not be blocked.

Note The AMF control VLANs and AMF management subnets can be manually changed.

With AMF enabled, the number of ACLs on the switches decreases from 2049 to 2048. If this is problematic and you are not using AMF, you can disable AMF, which will allow the previous maximum of 2049.

NTP and AMF

AMF uses NTP to synchronize the system clocks across nodes within the network. For this to operate, one or more external NTP servers must be configured on the network, and every node on the network must be configured to use the external server or servers.

Alternatively, you can configure an AlliedWare Plus device as the NTP master, but this NTP master must not be a member of the AMF network. Otherwise, NTP synchronization issues can occur.

To configure an AlliedWare Plus device as an NTP master, use the command:

```
awplus(config)# ntp master 11
```

The primary function of NTP within an AMF network is to ensure that time and date stamps on backups are consistent across member nodes within the backup. This is particularly important in an AMF network that has multiple AMF master nodes, to ensure that node recovery is performed with the most up-to-date backup.

Configuring NTP on the AMF network

Before you configure NTP on the AMF network, we recommend setting all nodes in the network to the same time, date, and timezone, to ensure NTP synchronization. To do this, create an AMF working-set of the whole network and set the date and time, for example:

```
awplus(config)# atmf working-set group all
awplus(config)# clock set 16:47:00 11 Sep 2014
awplus(config)# clock timezone utc plus 12
```

Once you have configured all nodes with the same time, date and timezone, configure the working-set of all nodes with the IP address of the NTP server, for example:

```
awplus(config)# ntp server 172.31.0.1
```

You can then check that the nodes have synchronized with the NTP server using the **show ntp status** command, for example:

```
awplus# show ntp status
```

```
awplus#show ntp status
Clock is synchronized, stratum 13, reference is 172.31.0.1
actual frequency is 7.1420 PPM, precision is 2**-18
reference time is d7bba834.19f1a68f (16:48:52.101 utc Thu Sep 11
2014)
clock offset is -1.286 msec, root delay is 2.237 msec
root dispersion is 45.213 msec
```

Configuring AMF

The following configuration example uses a simplified network to explain the steps required to configure AMF. Note that this example describes a full AMF network, but GS900MX/MPX switches can only be configured as AMF edge switches with a single uplink.

Figure 60-4: Simple AMF single master example

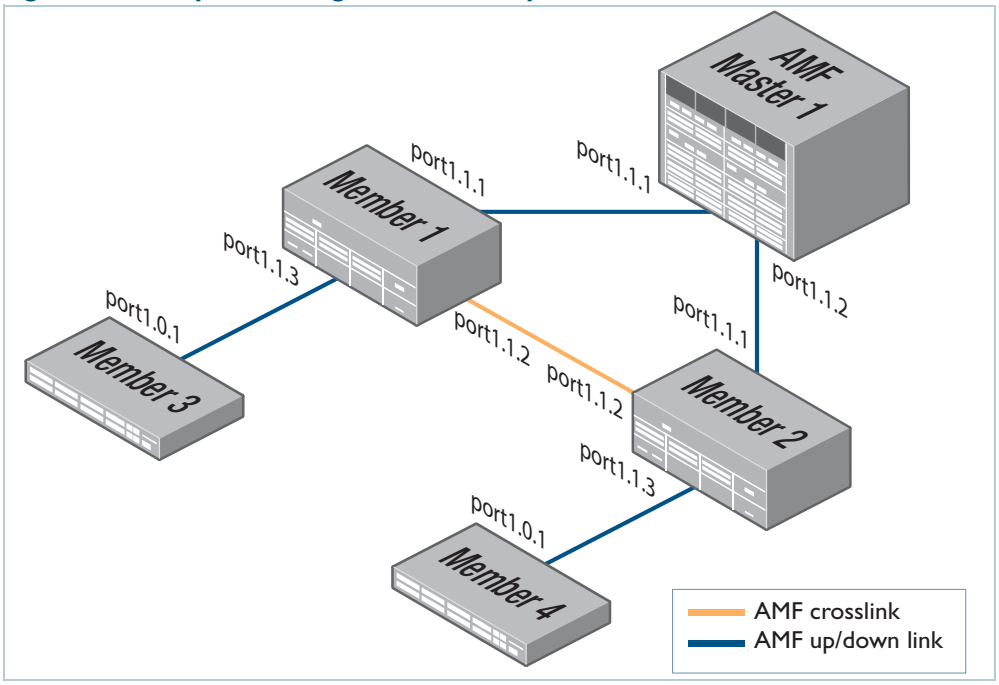


Table 60-2: Configure the AMF master node

Description	Prompt	Command
Step 1. Set the host name.		
Enter Global Configuration mode	`(awplus#)`	`configure terminal`
Set the host name	`awplus(config)#`	`hostname AMF_Master`
Note that host names are used as the AMF node name and **MUST BE UNIQUE** within the AMF network.		
Step 2. Set the AMF network name.		
Set the AMF network name.	`AMF_Master(config)#`	`atmf network-name atmf1`
Note that the AMF network name must be the same on all nodes within the AMF network, and the device must be *rebooted* before the AMF network name takes effect.		
Step 3. Configure the switch to be the AMF master.		
	`AMF_Master(config)#`	`atmf master`
An AMF network must have at least one master configured. A license is required for each AMF master in the AMF network. If an AT-SBx8100 with dual CFCs is configured as an AMF master a license is only required on the CFC master, as the license with be synchronized across CFCs. If an AT-SBx908 or AT-x930 Series switch is configured as an AMF master, a license is required to be installed on **all** stack members.		
Step 4. Configure the data VLANs.		
	`AMF_Master(config)#`	`vlan database`
	`AMF_Master(config-vlan)#`	`vlan 2-3`
Step 5. Configure ports as AMF-links.		
	`AMF_Master(config)#`	`interface port1.1.1-1.1.2`
	`AMF_Master(config-if)#`	`switchport atmf-link`
Step 6. Configure data VLANs on AMF-links as required.		
	`AMF_Master(config-if)#`	`switchport trunk allowed vlan add 2-3`
Step 7. Save the configuration and reboot the switch.		
	`AMF_Master#`	`copy running-config startup-config`
Building configuration...[OK]		
	`AMF_Master#`	`reload`
Are you sure you want to reboot the whole chassis? (y/n): y		

Table 60-3: Configure the first member node (Member1)

Description	Prompt	Command
Step 1. Set the host name.		
Enter Global Configuration mode	`(awplus#)`	`configure terminal`
Set the host name	`awplus(config)#)`	`hostname Member1`
Note that host names are used as the AMF node name and **MUST BE UNIQUE** within the AMF network.		
Step 2. Set the AMF network name.		
Set the AMF network name to atmf1.	`Member1(config)#`	`atmf network-name atmf1`
Note that the AMF network name must be the same on all nodes within the AMF network, and the device must be *rebooted* before the AMF network name takes effect.		
Step 3. Configure the data VLANs.		
Enter the VLAN Configuration mode	`Member1(config)#`	`vlan database`
Create VLANs 2 and 3	`Member1(config-vlan)#`	`vlan 2-3`
Step 4. Configure ports as AMF-links.		
Enter Interface Configuration mode for ports 1.1.1 to 1.1.3	`Member1(config)#`	`interface port1.1.1-1.1.3`
Configure these ports as AMF links	`Member1(config-if)#`	`switchport atmf-link`
Step 5. Configure data VLANs on the AMF-links as required.		
Set VLANs 2 to 3 to be data VLANs	`Member1(config-if)#`	`switchport trunk allowed vlan add 2-3`
Step 6. Configure AMF-crosslink.		
Enter the Interface Configuration mode for port 1.1.2	`Member1(config)#`	`interface port1.1.2`
Set this port to be an AMF-crosslink	`Member1(config-if)#`	`switchport atmf-crosslink`
	`Member1(config-if)#`	`switchport trunk native vlan none`
Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.		
Step 7. Save the configuration and reboot the switch.		
	`Member1#`	`copy running-config startup-config`
Building configuration...[OK]		
	`Member1#`	`reload`
Are you sure you want to reboot the whole chassis? (y/n):		`y`

Table 60-4: Configure the first member node (Member2)

Description	Prompt	Command
Step 1. Set the host name.		
Enter Global Configuration mode	awplus#)	configure terminal
Set the host name	awplus(config)#)	hostname Member2
Note that host names are used as the AMF node name and **MUST BE UNIQUE** within the AMF network.		
Step 2. Set the AMF network name.		
Set the AMF network name to atmf1.	Member2(config)#	atmf network-name atmf1
Note that the AMF network name must be the same on all nodes within the AMF network, and the device must be *rebooted* before the AMF network name takes effect.		
Step 3. Configure the data VLANs.		
Enter the VLAN Configuration mode	Member2(config)#	vlan database
Create VLANs 2 and 3	Member2(config-vlan)#	vlan 2-3
Step 4. Configure ports as AMF-links.		
Enter Interface Configuration mode for ports 1.1.1 to 1.1.3	Member2(config)#	interface port1.1.1-1.1.3
Configure these ports as AMF links	Member2(config-if)#	switchport atmf-link
Step 5. Configure data VLANs on the AMF-links as required.		
Set VLANs 2 to 3 to be data VLANs	Member2(config-if)#	switchport trunk allowed vlan add 2-3
Step 6. Configure AMF-crosslink.		
Enter the Interface Configuration mode for port 1.1.2	Member2(config)#	interface port1.1.2
Set this port to be an AMF-crosslink	Member2(config-if)#	switchport atmf-crosslink
	Member2(config-if)#	switchport trunk native vlan none
Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.		
Step 7. Save the configuration and reboot the switch.		
	Member2#	copy running-config startup-config
Building configuration...[OK]		
	Member2#	reload
Are you sure you want to reboot the whole chassis? (y/n):		y

Table 60-5: Configure the first member node (Member3)

Description	Prompt	Command
Step 1. Set the host name.		
Enter Global Configuration mode	`(awplus#)`	`configure terminal`
Set the host name	`awplus(config)#)`	`hostname Member3`
Note that host names are used as the AMF node name and **MUST BE UNIQUE** within the AMF network.		
Step 2. Set the AMF network name.		
Set the AMF network name to atmf1.	`Member3(config)#`	`atmf network-name atmf1`
Note that the AMF network name must be the same on all nodes within the AMF network, and the device must be *rebooted* before the AMF network name takes effect.		
Step 3. Configure the data VLANs		
Enter the VLAN Configuration mode	`Member3(config)#`	`vlan database`
Create VLANs 2 and 3	`Member3(config-vlan)#`	`vlan 2-3`
Step 4. Configure ports as AMF-links.		
Enter Interface Configuration mode for ports 1.0.1 to 1.0.3	`Member3(config)#`	`interface port1.0.1-1.0.3`
Configure these ports as AMF links	`Member3(config-if)#`	`switchport atmf-link`
Step 5. Configure data VLANs on the AMF-links as required.		
Set VLANs 2 to 3 to be data VLANs	`Member3(config-if)#`	`switchport trunk allowed vlan add 2-3`
Step 6. Configure AMF-crosslink.		
Enter the Interface Configuration mode for port 1.0.2	`Member3(config)#`	`interface port1.0.2`
Set this port to be an AMF crosslink	`Member3(config-if)#`	`switchport atmf-crosslink`
	`Member3(config-if)#`	`switchport trunk native vlan none`
Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.		
Step 7. Save the configuration and reboot the switch.		
	`Member3#`	`copy running-config startup-config`
Building configuration...[OK]		
	`Member3#`	`reload`
Are you sure you want to reboot the whole chassis? (y/n):		`y`

.

Table 60-6: Configure the first member node (Member4)

Description	Prompt	Command
Step 1. Set the host name.		
Enter Global Configuration mode	`(awplus#)`	`configure terminal`
Set the host name	`awplus(config)#)`	`hostname Member4`
Note that host names are used as the AMF node name and **MUST BE UNIQUE** within the AMF network.		
Step 2. Set the AMF network name.		
Set the AMF network name to atmf1.	`Member4(config)#`	`atmf network-name atmf1`
Note that the AMF network name must be the same on all nodes within the AMF network, and the device must be *rebooted* before the AMF network name takes effect.		
Step 3. Configure the data VLANs.		
Enter the VLAN Configuration mode	`Member4(config)#`	`vlan database`
Create VLANs 2 and 3	`Member4(config-vlan)#`	`vlan 2-3`
Step 4. Configure ports as AMF-links.		
Enter Interface Configuration mode for ports 1.0.1 to 1.0.3	`Member4(config)#`	`interface port1.0.1-1.0.3`
Configure these ports as AMF links	`Member4(config-if)#`	`switchport atmf-link`
Step 5. Configure data VLANs on the AMF-links as required.		
Set VLANs 2 to 3 to be data VLANs	`Member4(config-if)#`	`switchport trunk allowed vlan add 2-3`
Step 6. Configure AMF-crosslink.		
Enter the Interface Configuration mode for port 1.0.2	`Member4(config)#`	`interface port1.0.2`
Set this port to be an AMF crosslink	`Member4(config-if)#`	`switchport atmf-crosslink`
	`Member4(config-if)#`	`switchport trunk native vlan none`
Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.		
Step 7. Save the configuration and reboot the switch.		
	`Member4#`	`copy running-config startup-config`
Building configuration...[OK]		
	`Member4#`	`reload`
Are you sure you want to reboot the whole chassis? (y/n):		`y`

Verifying the AMF Network

To check that all nodes have joined the AMF network use the **show atmf** command on page 61.56 with the summary parameter. You can run this command from any node in an AMF network.

Figure 60-5: Checking AMF configuration using the show atmf summary command

```
AMF_Master#show atmf summary
ATMF Summary Information:
ATMF Status            : Enabled
Network Name           : atmf1
Node Name              : AMF_Master
Role                   : Master
Current ATMF Nodes     : 5
AMF_Master#
```

The **Current AMF Nodes** field in the output above shows that all 5 nodes have joined the AMF network.

Use the **show atmf nodes** command on page 61.80 to check information on individual nodes:

Figure 60-6: Output from the show atmf nodes command

```
AMF_Master#show atmf nodes
Node Information:
  * = Local device
 SC = Switch Configuration:
  C = Chassis   S = Stackable   N = Standalone
Node              Device            ATMF                          Node
Name              Type              Master     SC  Parent        Depth
-------------------------------------------------------------------
* AMF_Master      AT-SBx81CFC400      Y        C   none            0
  Member1         SwitchBlade x908    N        S   AMF_Master      1
  Member2         SwitchBlade x908    N        S   AMF_Master      1
  Member4         x510-52GTX          N        S   Member2         2
  Member3         x510-52GTX          N        S   Member2         2
 Current ATMF node count 5
```

Note that the *Parent* field in the output above refers to the parent *domain* and not the upstream device. In the example output above, Member2 is the domain controller for the parent domain for Member3 and Member4.

Use the **show atmf links** command on page 61.69 to check information on individual AMF links:

Figure 60-7: Checking output with the show atmf links command

```
switch1# show atmf links

ATMF  Links Brief:

Local    Link      Port    ATMF         Adjacent             Adjacent Link
Port     Type      Status  State        Node                 Ifindex  State
-------------------------------------------------------------------------------
sa1      Crosslink Up      TwoWay       Building_1           4501     Forwarding
1.0.1    Downlink  Up      Full         Bld1_Floor_1         5001     Forwarding
1.0.2    Downlink  Up      Full         Bld1_Floor_2         5003     Forwarding
1.0.3    Downlink  Up      Full         Bld2_Floor_1         6101     Forwarding
1.0.4    Crosslink Down    Init         *switch3                      Blocking

* = provisioned
```

Configuring Multiple Nodes at the Same Time: the Unified CLI

The unified CLI is a central component of AMF. It provides you with a configuration and display interface that can control a selected collection of nodes, or the entire AMF network, from a single point. This control is provided through the **atmf working-set** command.

The working-set

An AMF working-set is a set of nodes that can be collectively configured from a single device. Working sets can either **arbitrarily user defined** or **automatically created** (a pre-defined working-set). Specifying or selecting a working-set enables CLI commands to be executed on all nodes within the working-set by using a single command. A working-set can be defined, selected, and configured from any node within an AMF network.

Note

For security reasons you can limit the action of working sets by applying "restrictive login." For more information, see **"atmf restricted-login" on page 61.47**

By default, when you first log into a node that is part of an AMF network, you are implicitly placed into the working-set group **local**, a working-set that contains only the local node. In this instance the CLI prompt when you log in will be either:

- the host-name, if one has been assigned, or
- in the case of a new node in safe mode, a host name based on its MAC address followed by the usual prompt (> or #)

```
Node1> enable
Node1#
```

To create a working set containing a set of nodes use the command **atmf working-set** followed by a comma separated list of the nodes you wish to control. Whenever you select a working set containing any nodes other than the local device, the CLI prompt will display the AMF network name, followed by the number of nodes contained in the working set in square brackets (**atmf1[2]** in the following example).

```
Node1# atmf working-set Node1,Node2
 Node1,Node2
                    Working set join
atmf1[2]#
```

To return to just controlling the local device from any other working set, use the command **atmf working-set group local**.

Working-Set Groups

AMF contains the ability to have working-set groups, so that it is not always necessary to use a comma separated list to specify a working-set.

AMF working-set groups can be split into two types:

- Automatic
- User-defined

Automatic working-set groups

There are three automatic working-set groups that will exist on every AMF network:

1. *All*—all nodes within the AMF network.
2. *Current*—the current working-set of nodes. This group is useful for adding additional nodes to the current working-set.
3. *Local*—the local device

In any AMF network there will also be a number of other automatic working-set groups that are dependent on the platform types which exist within the network. To see the platform dependent automatic working-set groups that exist on the AMF network use the command **show atmf group** with the automatic parameter:

```
x908_VCS_1#show atmf group members automatic

Retrieving Automatic groups from:
x510_1 Master x908_VCS_2 x908_VCS_1

ATMF Group membership

Automatic        Total
Groups           Members   Members
poe              1         Master
x510             1         x510_1
SBx8100          1         Master
x900             2         x908_VCS_2 x908_VCS_1
```

To select a working-set group use the **atmf working-set** command with the group parameter, followed by the group name. You can specify a single group, a comma-separated list of groups, or a comma-separated list of individual nodes followed by a comma-separated list of groups:

```
x908_VCS_1# atmf working-set x510_1,x510_2 group x900

 x510_1, x510_2, x908_VCS_1, x908_VCS_2

                    Working set join

atmf1[4]#
```

If you specify a partially invalid working-set node list or group list, only the valid nodes or groups will join the working set. If you specify a completely invalid working-set, you will create a working-set containing no nodes. The switch will generate a warning message to alert you that the current working-set is empty:

```
atmf1[3]# atmf working-set group x511

% Warning - working set is now empty

atmf1[0]#
```

User-defined working-set groups

In addition to the automatic working-set groups, you can create user-defined groups for arbitrary sets of nodes that you wish to group together, for example, all AMF master nodes.

To create a user-defined working-set group:

1. Create a working-set containing the desired nodes.
2. In global configuration mode use the command **"atmf group (membership)" on page 61.19**.

```
Master# atmf working-set Master1,Master2

Master1,Master2

                    Working set join

atmf1[2]# conf t

atmf1[2]# atmf group new-group-name
```

You can see all user-defined working-set groups that exist on the AMF network with the command **"show atmf group members" on page 61.67**:

```
x908_VCS_1#show atmf group members user-defined

Retrieving Automatic groups from:
x510_1 Master1, Master2, x908_VCS_2 x908_VCS_1

ATMF Group membership

User-defined     Total
Groups           Members   Members
-----------------------------------------------------------------
Masters          2         Master1 Master2

Master#
```

Executing Commands on Working-Sets

Executing commands on a working-set of nodes is very similar to executing commands on a single AlliedWare Plus device.

When a command is executed that is valid for all nodes within the working-set, the output is displayed for each of the nodes separately. However, output will be grouped when it is the same for more than one node.

Here is an example output of the **show arp** command run from a working-set:

```
atmf1[4]#show arp
=======
Master:
=======

 IP Address     MAC Address      Interface    Port       Type
 172.31.0.1     eccd.6d7d.a542   ATMF         sa1        dynamic
 172.31.0.3     0000.cd2b.0329   ATMF         sa1        dynamic
 172.31.0.10    0000.cd37.0163   ATMF         sa1        dynamic

=======
x510_1:
=======

 IP Address     MAC Address      Interface    Port       Type
 172.31.0.2     eccd.6d03.10f9   ATMF         sa4        dynamic

===========
x908_VCS_1:
===========

 IP Address     MAC Address      Interface    Port       Type
 172.31.0.2     0000.cd37.1050   ATMF         sa1        dynamic

===========
x908_VCS_2:
===========

 IP Address     MAC Address      Interface    Port       Type
 172.31.0.2     0000.cd37.1050   ATMF         sa3        dynamic

atmf1[4]#
```

Invalid working-set commands

Some commands can only be executed on *certain* nodes within the working-set. In this case the command will be attempted on all nodes within the working-set. For any node for which the command is not valid, the command execution will fail and the output displayed will indicate the nodes on which the command succeeded and nodes on which the command failed.

Below is example output from the **show card** command run from a working-set, which is only a valid command for the SBx8100 series switches.

```
atmf1[4]# show card
=======
Master:
=======

Slot Card Type        State
-----------------------------------------------
1    AT-SBx81GP24     Online
2    AT-SBx81GP24     Online
3    AT-SBx81GP24     Online
4    AT-SBx81XS6      Online
5    AT-SBx81CFC400   Online (Active)
6    -                -
7    -                -
8    -                -
9    -                -
10   -                -
11   -                -
12   -                -
-----------------------------------------------
==============================
x510_1, x908_VCS_1, x908_VCS_2:
==============================
% Invalid input detected at '^' marker.
```

Sub-configuration limitations for some nodes in a working-set

There will be some instances where a sub-configuration mode is only valid for some of the nodes in the working-set. One example of this would be when entering interface configuration mode for a port that exists on some members of the working-set and not on others. For example:

```
              atmf1[4]# conf t
       atmf1[4](config)# int port1.1.1
% Can't find interface port1.1.1
  atmf1[4:2](config-if)# conf t
```

In the example above the interface **port1.1.1** exists on two of the nodes in the working-set, but does not exist on nodes “Master” or “x510_1”. The interface configuration mode fails for these nodes, and a warning message is output to indicate this. Inside the square brackets, the first number indicates the total number of nodes in the working-set, and the second number indicates the number of nodes in the sub-configuration mode that has been entered. Any configuration commands configured in this mode will only be executed on the nodes that successfully entered the sub-configuration mode.

Entering **exit** while in this mode will return to global configuration mode for all nodes within the working-set:

```
  atmf1[4:2](config-if)# exit
       atmf1[4](config)# (config)#
```

Interactive Commands

It is inappropriate to execute **interactive** commands simultaneously across multiple nodes within a working-set. These commands can only be executed on the local node working-set or on a working-set with a single member.

When any interactive commands are entered from within a working-set they will give an error:

```
atmf1[4]# ping 4.2.2.1
% Working set must contain only single node for this command
```

The list of current interactive commands, including any optional parameters, are:

- ping
- mtrace/mstat
- traceroute
- boot system
- boot configuration-file
- banner login
- tcpdump
- edit
- copy
- mail
- move
- terminal monitor

AMF Backups

AMF backups are a valuable part of AMF network operation. They are the mechanism by which AMF master nodes update their records of the AMF network. By default, AMF master nodes are configured to perform automatic scheduled backups of the entire AMF network once per day at 3.00am. AMF backups can be stored on **remote file servers** or **external removable media** such as USB sticks or SD cards. These backup files can be used in the recovery of a failed node.

Note that this feature will operate only on AMF master nodes.

Using External Media Storage

If storing data on external media, it is a requirement that all AMF masters have external removable media installed with sufficient capacity to hold all of the relevant files stored in the Flash on every node in the AMF network.

Typically a *4 GB* capacity external media storage would be of sufficient size to hold backups for a *40 node* AMF network.

The AMF node backup system has been designed such that the external media used to store the backup data can still be used to store other data. However, care needs to be taken to ensure that enough space is reserved for future AMF backups.

- AMF requires up to 128 MB backup space for SBx8100 nodes and up to 64 MB backup space for other nodes. The output from the **show atmf backup** command on page 61.60 will provide warnings if capacity on the backup media falls below a safe level.

Here is an output example from the **show atmf backup** command showing a backup media space warning:

Figure 60-8: Output showing backup media space warning

```
master1#show atmf backup

Scheduled Backup ...... Disabled
  Schedule ............ 1 per day starting at 12:45
  Next Backup Time .... 25 May 2014 12:45
Backup Media .......... SD (Total 3827.0MB, Free 7.1MB)
                        WARNING: Space on backup media is below 64MB
Current Action ........ Idle
  Started ............. -
  Current Node ........ -
```

Safe removal of external storage media

Removing external storage media, or rebooting the master node, while an AMF backup is underway could potentially cause corruption to files in the backup. Although files damaged as a result of mishandling backup media will be replaced during the next backup cycle, if the file system on the media becomes damaged, it may require reformatting before being inserted into the AMF master. To avoid any damage to the AMF backup files or file system, we recommend that the following procedure be followed before rebooting or removing any external storage media from an AMF master.

1. Disable backups to prevent a scheduled backup from occurring while the card is being removed.

2. Terminate any backup already in process.

3. Verify that it is safe to remove the media by checking that backups are disabled and that there are no backups currently in progress.

Figure 60-9: Example of the safe external storage media removal procedure

```
master1#conf t

master1(config)#no atmf backup enable
master1(config)#exit
master1#atmf backup stop
master1#show atmf backup

Scheduled Backup ...... Disabled
  Schedule ............ 1 per day starting at 12:45
  Next Backup Time .... 25 May 2014 12:45
Backup Media .......... SD (Total 3827.0MB, Free 3257.1MB)
Current Action ........ Idle
  Started ............. -
  Current Node ........ -
```

Once the media has been reinstalled, ensure that the backup scheduler is re-enabled.

Performing a Manual Backup

Whenever a new device is physically added to the AMF network as a provisioned node, we advise that you perform a manual backup from the AMF master.

To perform a manual backup of the entire AMF network, on the AMF master enter the command **atmf backup now** command on page 61.8:

```
Master1# atmf backup now
Master1(config)# atmf backup enable
Master1(config)# exit
```

To check the status of the AMF backup use the **show atmf backup** command on page 61.60.

Figure 60-10: Example output from the show atmf backup command entered during a backup

```
AMF_Master#show atmf backup
Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 14 Dec 2013 03:00
Backup Media .......... USB (Total 3692.6MB, Free 1782.7MB)
Current Action ........ Doing manual backup
  Started ............. 13 Dec 2012 05:20
  Current Node ........ Member1
Node Name                      Date         Time      In ATMF  On Media  Status
-------------------------------------------------------------------------------
AMF_Master                     13 Dec 2012  05:20:16  Yes      Yes       Good
Member1                        -            -         Yes      Yes       -
Member2                        -            -         Yes      No        -
Member3                        -            -         Yes      No        -
Member4                        -            -         Yes      No        -
```

Below is example output from the **show atmf backup** command entered after the backup has completed.

Figure 60-11: Example output from the show atmf backup command entered after backup was completed

```
AMF_Master#show atmf backup
Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 13 Dec 2013 03:00
Backup Media .......... USB (Total 3692.6MB, Free 1651.1MB)
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

Node Name                      Date         Time     In ATMF  On Media  Status
-------------------------------------------------------------------------------
ATMF_Master                 13 Dec 2013  05:20:16  Yes      Yes       Good
Member1                     13 Dec 2013  05:20:27  Yes      Yes       Good
Member2                     13 Dec 2013  05:20:40  Yes      Yes       Good
Member3                     13 Dec 2013  05:20:52  Yes      Yes       Good
Member4                     13 Dec 2013  05:21:08  Yes      Yes       Good
```

Note that the file system used by the AMF backup does not support the backing up of files that have the same name but have different case (e.g. “test.txt” and “TEST.txt”), and only **one** of these files will be stored in the backup. For this reason we recommend that all files on a node be given unique file names.

Backing up to Remote Servers

System backup data can be held on up to two remote backup servers rather than on the master node’s external media. These servers are used for both backup and recovery.

Each AMF master supports a maximum of two remote file servers. The remote backup file servers are mounted on the Master’s file system using SSH and appear as folders.

Configuring a backup to a remote server

First configure the servers. After you have configured the servers you can check the backup media, location, log details and server status using the **show atmf backup** command. You can also manually synchronize the contents of an active server and other configured servers, if required. The following steps show how to set up two backup servers:

1. Use the command **“atmf backup server” on page 61.10** for backup server 1

   This command configures a remote file server(s) as the destination for AMF backups.

   Configuration of a remote server will switch the backup to remote server functionality and disable any further backup to external media. Use the **no** variant of this command to remove the destination servers and revert to backup from external media.

   Note that if no servers are configured, the backup will go to external media. If no servers are configured and no external media exists, no backup will occur.

2. Repeat step (1) for backup server 2
   You should now have two file servers configured to backup your network.

3. Use the **“atmf backup now” on page 61.8** to force a manual backup of your network.

   Note This step is optional. Alternatively you could wait until the next scheduled back occurs.

4. Use the command **“show atmf backup” on page 61.60**.

If you forced a manual backup, you will probably want to display the location and state of each configured file server. The display from this command also shows diagnostic results that test connectivity to each server by using the optional `server-status` parameter.

Below is example output from the **show atmf backup** command showing the configuration of two remote backup file servers.

Figure 60-12: Output from the show atmf backup command showing the configuration of two remote backup file servers

```
x900a#show atmf backup
  Scheduled Backup ...... Enabled
    Schedule ............ 24 per day starting at 14:25
    Next Backup Time .... 19 May 2014 11:25
  Backup Bandwidth ...... Unlimited
  Backup Media .......... FILE SERVER (Total 503837.5MB, Free 186818.0MB)
  Server Config ..........
    Synchronization ..... Synchronized
      Last Run .......... 19 May 2014 11:09:50
     1 .................. Configured   (Mounted)
      Host ............... 10.36.150.54
      Username ........... user_1
      Path ............... temp/x900a_1
      Port ............... -
    * 2 .................. Configured   (Mounted, Primary)
      Host ............... tb165.test.com
      Username ........... user_2
      Path ............... temp/x900a_2
      Port ............... -
  Current Action ........ Idle
    Started ............. -
    Current Node ........ -
-------------------------------------------------------------------------------
  Node Name                      Date         Time      In ATMF  On Media  Status
       Synchronization           Date         Time      From Id  To Id     Status
  ---------------------------------------------------------------------------
-
  x210a                          19 May 2014  11:09:37  Yes      Yes       Good
                                 19 May 2014  11:09:46  2        1         Good
  x610a                          19 May 2014  11:09:17  Yes      Yes       Good
                                 19 May 2014  11:09:19  2        1         Good
  x610b                          19 May 2014  11:09:49  Yes      Yes       Good
                                 19 May 2014  11:09:49  2        1         Good
  x610c                          19 May 2014  11:09:20  Yes      Yes       Good
                                 19 May 2014  11:09:20  2        1         Good
  x610d                          19 May 2014  11:09:19  Yes      Yes       Good
                                 19 May 2014  11:09:19  2        1         Good
  x900a                          19 May 2014  11:09:49  Yes      Yes       Good
                                 19 May 2014  11:09:50  2        1         Good
  x908stk                        19 May 2014  11:09:47  Yes      Yes       Good
                                 19 May 2014  11:09:48  Yes      Yes       Good
```

You can use the **show atmf backup** with the parameter `server-status` to display the results of the diagnostics that test connectivity to each server:

Figure 60-13: Output from the show atmf backup command showing diagnostic test results from each server

```
Master1#sh atmf backup server-status
 Id  Last Check  State
  -------------------------------------
 1      186 s  File server ready
  2          1 s  SSH no route to host
```

Node Recovery

Automatic Node Recovery

With AMF, you can replace a failed node with another device and let AMF automatically load the appropriate configuration onto the replacement device.

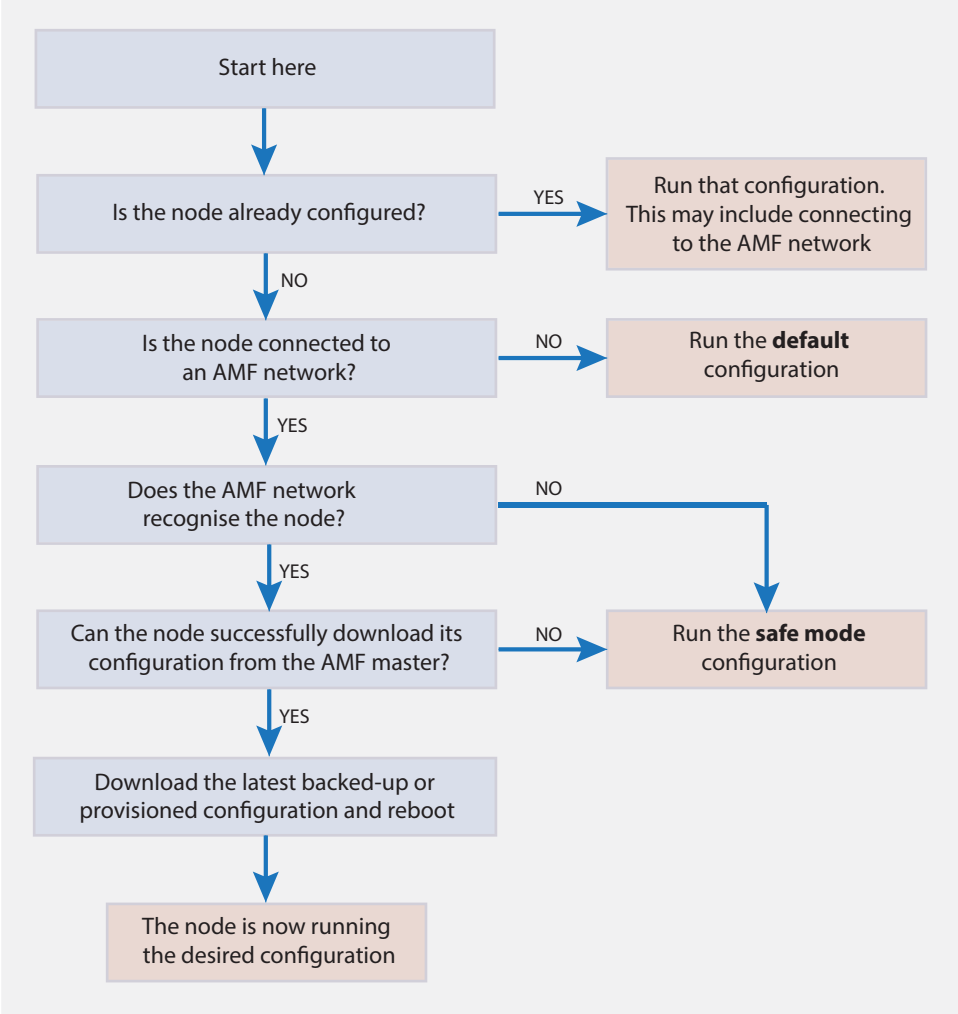
For this to work, the replacement device must have no configuration file. This means it must be either:

- a factory-new device, or
- a used device that has been returned to a "clean" state (see **"Restoring a Node to a "Clean" State" on page 60.32**)

To replace a failed device with a new device of a different platform or with a different node name, you need to provision the network to expect the new device. See **"Node Provisioning" on page 60.42**.

When a switch boots up, it goes through the process in the following flowchart to determine what configuration to use. This flowchart indicates when automatic node recovery will be successful.

Figure 60-14: How a switch determines which configuration to use



Automatic node recovery is not intended to recover multiple nodes simultaneously. If multiple nodes have failed, recover them one at a time.

Caution **Do not make any changes to the device's configuration while a node recovery is underway. A log message will appear on the console or other VTY session indicating when recovery has finished (whether successfully or with errors). This message can also be found by viewing the log with the show log command.**

Figure 60-15: Example log output showing automatic node recovery

```
23:03:15 awplus ATMF[863]: ATMF network detected
23:03:15 awplus ATMF[863]: ATMF safe config applied (forwarding disabled)
23:03:25 awplus ATMF[863]: Shutting down all non ATMF ports
23:03:26 x510_1 ATMF[863]: Automatic node recovery started
23:03:26 x510_1 ATMF[863]: Attempting to recover as x510_1
23:03:26 x510_1 ATMF[863]: Checking master node availability
23:03:32 x510_1 ATMF[863]: Master has joined. 2 members in total.
23:03:32 x510_1 ATMF[863]: x908_VCS_2 has joined. 3 members in total.
23:03:32 x510_1 ATMF[863]: x908_VCS_1 has joined. 4 members in total.
23:03:37 x510_1 ATMFFSR[2950]: Retrieving recovery data from master node Master
23:05:18 x510_1 ATMFFSR[2950]: File recovery from master node succeeded. Node will
now reboot
Flushing file system buffers...
Unmounting any remaining filesystems...
Restarting system.
```

Recovery progress indication

This is a visual feature that displays the recovery status during automatic recovery. This feature uses two distinct flash patterns to indicate the following states:

Recovery State	LED Indication (green)
Recovery in progress	Progressive strobing of all port LEDs.
Recovery failure	All port LEDs alternating on and off, flashing at the same time.

When using this feature during a recovery failure, you can turn off the failure-alert indication and return the port LEDs to their normal running state. To do this, use the command **"atmf recover led-off" on page 61.45**.

You can repeat this process until the recovery failure has been fixed.

Note that the Find me and ecofriendly LED features cannot be used while AMF recovery progress indication is active.

Restoring a Node to a "Clean" State

When replacing a failed device, your replacement device should be one of the following types, in order for AMF automatic node recovery to work:

- A factory-new device
- A used device that has been returned to a "clean" state

A clean device is one that has had its previous configuration components removed. The process of cleaning is required when replacing a failed device with one that, although in working condition, has been used previously and still retains components of its previous configuration.

If you keep on-site spares, store them with clean configurations and current releases. When you upgrade your network to a new AlliedWare Plus version, we recommend you upgrade your spare devices too.

To clean up a previously used device, use the **atmf cleanup** command on page 61.14. This command erases all data from NVS and Flash **apart from**:

- The boot release file (a .rel file) and its release setting file
- v1 license files /.configs/.swfeature.lic
- v2 license files /.configs/.sw_v2.lic

The device is then rebooted to put it into a clean state. The device can then be used for automatic node recovery.

Any other user files that remain in Flash will be overwritten during the automatic recovery process. If there are any files stored in the Flash of the replacement device that need to be retained, back these files up prior to installing the device into the AMF network.

Manual Node Recovery

There are certain situations where automatic recovery may fail. Automatic recovery has been designed to be cautious in its approach to recovering nodes for reasons such as:

- The backup stored on the AMF master not having a “Good” status
- The replacement device having a release of the AlliedWare Plus Operating System installed on it that is old enough to be incompatible with AW+ on the neighbor or the master.

When these situations occur, automatic node recovery will fail.

In this failed state, the replacement device will have the AMF safe configuration mode applied (see **“AMF Safe Configuration Procedures” on page 60.35**). After investigating the failure and taking remedial action, you may want to initiate manual node recovery. To do this, enter the following command:

```
amf1# atmf recover {<node_name>} {<master_node_name>}
```

where:

- **node_name** is the host name of the device you wish to recover.
- **master_node_name** is the host name of the AMF master that contains the backup you want to use for the recovery.

The manual recovery command will bypass the usual checks performed by automatic node recovery. Make sure that the backup configuration stored on the specified AMF master is correct before you execute the command.

If you attempt to manually recover a node with the backup file of a node from a **different platform**, the release file from the backup will be incompatible and won’t be copied to the replacement device. Instead, the existing release on the replacement device will be used, in order to ensure the device can join the AMF network and function correctly.

Figure 60-16: Example output showing manual recovery

```
amf1#atmf recover x510_1 Master
This command will erase ALL flash contents.  Continue node recovery? (y/n)y
Manual node recovery successfully initiated
x510_1#23:15:32 x510_1 ATMFFSR[8477]: Retrieving recovery data from master node
Master
23:17:17 x510_1 ATMFFSR[8477]: Manual node recovery completed
x510_1#
```

Node Recovery on VCStacks

Node recovery on VCStacks that are part of an AMF network is somewhat different to node recovery of standalone devices.

This is because VCStack has its own node recovery mechanism that has different requirements to AMF.

In the extremely unlikely situation of needing to replace an entire VCStack that is a member of an AMF network, you can use AMF automatic node recovery to first recover Stack ID 1, which will become the VCStack master.

The replacement device which will become the VCStack master must be a clean unit (see **"Restoring a Node to a "Clean" State" on page 60.32**).

The procedure for recovering an entire stack is as follows:

1. Connect a clean device to the AMF network, and power it on. The connections into the AMF network should be between the appropriately configured AMF links on the neighboring node, and the ports previously configured as AMF links in the backup for the failed node configuration.
2. The AMF network should detect the replacement device and begin automatic node recovery. Wait until automatic node recovery completes, then check that the replacement device has come up correctly as VCStack ID 1, and that the configuration is correct.
3. Configure the next replacement device as VCStack ID 2. Ensure it is installed with a compatible release and the same set of licenses that exist on ID 1. Connect the VCStack cables and power it on.
4. VCStack ID 1 should detect ID 2 and synchronize the configuration and firmware release. Once this has completed, check that the VCStack has formed correctly, and then connect the remaining network connections.

For any additional VCStack members, repeat the last two steps, ensuring that the VCStack ID is set to the next sequential value for each additional device that is added to the VCStack.

For more information on VC Stacking, see:

- **"VCStack Introduction" on page 81.2**
- **"Replacing a stack member" on page 81.16**

AMF Safe Configuration

If AMF automatic node recovery fails, AMF contains a safety net feature that puts the replacement node into a safe configuration state. This is to prevent an unconfigured device from joining the network and creating loops.

Detecting AMF Safe Configuration Operation

A log message will be generated when AMF safe configuration is applied. This message will appear in the log some time after the startup sequence.

The message will also be output to the console or any connected VTY session.

AMF Safe Configuration Procedures

The procedures for AMF safe configuration are shown below:

- A special VLAN is created in the disabled state and given the name atmf_node_recovery_safe_vlan. The VID of this VLAN is determined dynamically to ensure that it does not conflict with either of the AMF management VLANs, or any other VLANs that are detected on the AMF network.
- All ports are removed from their default VLAN membership (VLAN 1).
- All ports are set as tagged members of the safe VLAN.
- Additionally, all ports that are not an AMF link or cross-link are shut down. The links and crosslinks are detected by AMF and added to the dynamic configuration. This is done to ensure correct behavior of static aggregators and Layer 3 protocols configured on the neighboring devices.

Figure 60-17: Example output from the show vlan command with the brief parameter set for a device in AMF safe configuration mode

```
awplus#sh vlan brief

VLAN ID  Name            Type    State   Member ports   (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======================================
1       default          STATIC  ACTIVE
4090    atmf_node_recovery_safe_vlan
                         STATIC  SUSPEND port1.0.1(t)  port1.0.2(t)  port1.0.3(t)
                                         port1.0.4(t)  port1.0.5(t)  port1.0.6(t)
                                         port1.0.7(t)  port1.0.8(t)  port1.0.9(t)
                                         port1.0.10(t) port1.0.11(t)
                                         port1.0.12(t) port1.0.13(t)
                                         port1.0.14(t) port1.0.15(t)
                                         port1.0.16(t) port1.0.17(t)
                                         port1.0.18(t) port1.0.19(t)
                                         port1.0.20(t) port1.0.21(t)
                                         port1.0.22(t) port1.0.23(t)
                                         port1.0.24(t)
```

Figure 60-18: Example output from the show running-config command for a device in AMF safe configuration mode

```
awplus#show running-config
...
!
vlan database
 vlan 4090 name atmf_node_recovery_safe_vlan
 vlan 4090 state disable
!
interface port1.0.1-1.0.4
 shutdown
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 4090
 switchport trunk native vlan none
!
interface port1.0.5
 switchport
 switchport atmf-link
 switchport mode trunk
 switchport trunk allowed vlan add 4090
 switchport trunk native vlan none
!
interface port1.0.6-1.0.24
 shutdown
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 4090
 switchport trunk native vlan none
!
...
```

Undoing an AMF Safe Configuration

If your node has had AMF safe configuration applied, you can use normal CLI configuration commands to modify the running-configuration to whatever configuration is required.

See below for an example of returning a device from AMF safe configuration mode to having default VLAN and port settings. Note that in this example a 24-port device has been used.

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.24
awplus(config-if)# switchport trunk native vlan 1
awplus(config-if)# switchport trunk allowed vlan remove 4090
awplus(config-if)# switchport mode access
                % port1.0.5 has ATMF link configured so
                its mode cannot be changed
```

```
awplus(config-if)# no shutdown
awplus(config-if)# exit
awplus(config-if)# vlan database
awplus(config-if)# no vlan 4090
awplus(config-if)# end
```

In order to retain connectivity to the AMF network, AMF link and crosslink settings should not be changed. In the example above you can see that port1.0.5 is an automatically configured AMF link. You can also see the error message indicating it was skipped by the **"switchport mode access" on page 17.16**. This is because AMF links must be in trunk mode.

Caution

No changes should be made to the device's configuration while a node recovery is underway. A log message will appear on the console or other logged in session indicating when recovery has finished (whether successfully or with errors). This message can also be found by viewing the log with the command "show log" on page 10.37.

Rolling-Reboot Firmware Upgrade

The rolling-reboot firmware upgrade feature enables nodes within an AMF network to be rebooted and upgraded in a rolling sequence so that downtime and management overheads are minimized. First, specify a set of nodes within the AMF network using the **atmf working-set** command, then use the **atmf reboot-rolling** command. All nodes in the specified working-set will be rebooted and upgraded one by one, starting with the nodes furthest from the core domain, and ending with nodes closest to, or in, the core domain.

Once the rebooted node has finished running its configuration and has brought its ports up, it re-joins the AMF network and the next node in the working-set is rebooted and upgraded.

Note The **atmf rolling-reboot** command can also be used to reboot a set of nodes without upgrading the firmware.

To upgrade firmware, a download URL can be selected from any media location.

Supported media locations include:

- flash:
- card:
- usb:
- tftp:
- scp:
- http:

The latest compatible release for a node will be selected from one of these locations. Several checks need to be performed to ensure the upgrade will succeed. This includes checking that the current node release boots from Flash and that there is enough space in Flash on this node. The new release name is updated using the **boot system backup** command. The old release will become the backup release file.

Note that if the release file is to be copied from a remote location (e.g. via TFTP or HTTP), the URL should specify the exact release filename without using wild card characters.

The node is rebooted and the new software version will be used. On bootup, the software release is verified. Should an upgrade fail, the upgrading unit will fail back to its old software version. At the completion of this command, a report is run showing the release upgrade status of each node.

The **force** parameter enforces a node reboot, even though the node may not be suitable for upgrading software. This command can take a significant amount of time to complete.

Note Rolling-reboot firmware upgrades can be performed on a working-set that includes the controlling node, although in this instance the user will not be presented with a summary report upon completion.

Here is an example of a Rolling-reboot firmware upgrade summary report:

```
================================================================================
ATMF Rolling Reboot Complete
Node Name   Reboot Status    Release Name                Release Status
--------------------------------------------------------------------------------

Node1       Rebooted         x510-main-20121018-2.rel    Upgraded

Node2       Rebooted         x900-main-20121018-2.rel    Upgraded

Node3       Rebooted         x900-main-20121018-2.rel    Upgraded

Node4       Rebooted         x510-main-20121018-2.rel    Upgraded
================================================================================
```

Performing a Rolling-Reboot Upgrade

To perform a Rolling-reboot firmware upgrade on all nodes in the AMF network, first select all nodes using the default working-set group **all**:

```
SBx8100# atmf working-set group all

SBx8100, SBx908-VCS1, SBx908-VCS2, x510_1, x510_2:

Working set join
```

Next, using the **atmf reboot-rolling** command, specify the path to the release files to use for the upgrade. In the following example the release files are stored on the external USB storage media installed in the node controlling the Rolling-reboot firmware upgrade, in a directory called "rel". Note that because the node controlling the Rolling-reboot firmware upgrade is included in the nodes to be upgraded, a message is output indicating that no summary will be available on completion.

```
csg_vcf[5]#atmf reboot-rolling usb:/rel/*.rel
Retrieving data from SBx8100
Retrieving data from SBx908-VCS2
Retrieving data from x510_1
Retrieving data from x510_2
Retrieving data from SBx908-VCS1

ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)  New Release File           Status
-------------------------------------------------------------------
x510_2              9          x510-main-20121203-1.rel   Release ready
x510_1              6          x510-main-20121203-1.rel   Release ready
SBx908-VCS1         9          x900-main-20121203-1.rel   Release ready
SBx908-VCS2         9          x900-main-20121203-1.rel   Release ready
SBx8100             11         SBx81CFC400-main-20121203  Release ready
                                 -1.rel
% The controlling node (SBx8100) is included in the
rolling reboot and will be rebooted last.
No summary will be available on completion.
Continue upgrading releases ? (y/n):
===================================================================
Copying Release    : x510-main-20121203-1.rel to x510_2
Updating Release   : x510-main-20121203-1.rel information on x510_2
===================================================================
ATMF Rolling Reboot: Rebooting x510_2
===================================================================
02:11:32 SBx8100 ATMF[1973]: x510_2 has left. 4 members in total.

% x510_2 has left the working-set
02:13:30 SBx8100 ATMF[1973]: x510_2 has joined. 5 members in total.
Reboot of x510_2 has completed
```

Although in this example no summary report was generated, you can refer to the progress messages output on the console to confirm that the upgrades were successful. You can also use the **atmf working-set** and the **show boot** commands to confirm the current boot image for each node in the AMF network.

```
================================================================
Copying Release    : x510-main-20121203-1.rel to x510_1
Updating Release   : x510-main-20121203-1.rel information on x510_1
================================================================
ATMF Rolling Reboot: Rebooting x510_1
================================================================
02:14:13 SBx8100 ATMF[1973]: x510_1 has left. 4 members in total.

% x510_1 has left the working-set
02:15:53 SBx8100 ATMF[1973]: x510_1 has joined. 5 members in total.
Reboot of x510_1 has completed

================================================

Copying Release    : x900-main-20121203-1.rel to SBx908-VCS1
Updating Release   : x900-main-20121203-1.rel information on SBx908-VCS1
================================================================
ATMF Rolling Reboot: Rebooting SBx908-VCS1
================================================================
02:19:02 SBx8100 ATMF[1973]: x510_1 has left. 4 members in total.
02:19:02 SBx8100 ATMF[1973]: SBx908-VCS1 has left. 3 members in total.

% SBx908-VCS1 has left the working-set
02:20:48 SBx8100 ATMF[1973]: SBx908-VCS1 has joined. 4 members in total.
Reboot of SBx908-VCS1 has completed
02:20:51 SBx8100 ATMF[1973]: x510_1 has joined. 5 members in total.
================================================================
Copying Release    : x900-main-20121203-1.rel to SBx908-VCS2
Updating Release   : x900-main-20121203-1.rel information on SBx908-VCS2
================================================================
ATMF Rolling Reboot: Rebooting SBx908-VCS2
================================================================
02:21:54 SBx8100 ATMF[1973]: x510_2 has left. 4 members in total.
02:21:54 SBx8100 ATMF[1973]: SBx908-VCS2 has left. 3 members in total.

% SBx908-VCS2 has left the working-set
02:23:35 SBx8100 ATMF[1973]: SBx908-VCS2 has joined. 4 members in total.
Reboot of SBx908-VCS2 has completed
================================================================
Copying Release    : SBx81CFC400-main-20121203-1.rel to SBx8100
02:23:39 SBx8100 ATMF[1973]: x510_2 has joined. 5 members in total.
Updating Release   : SBx81CFC400-main-20121203-1.rel information on SBx8100
================================================================
ATMF Rolling Reboot: Rebooting SBx8100
================================================================
02:24:07 SBx8100 ATMF: reboot-rolling Rebooting SBx8100 at request of user manager.
```

Node Provisioning

You can pre-configure, or provision, a port for a future node before the node is added to the network. A provisioned node can be created as a new unique entity, or can be cloned using the backup data from an existing node. When you connect the new node to the provisioned port in the AMF network, its configuration is loaded from the information stored in the backup media.

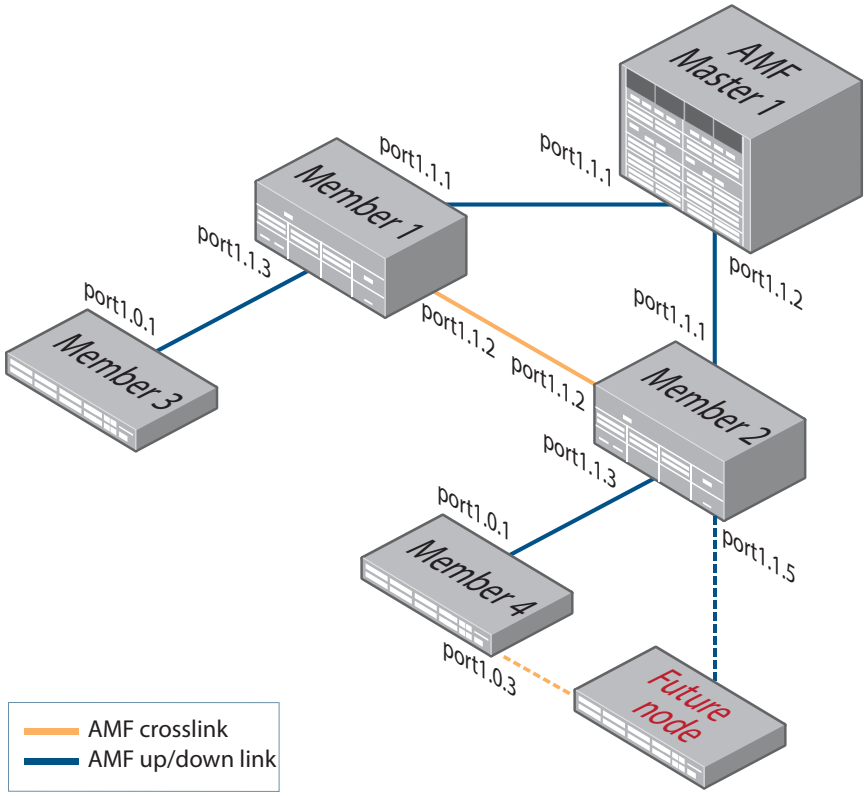
AMF commands are used to create and configure a provisioned node and to specify the port(s) that the node is expected to appear on.

When to use node provisioning

Node provisioning can be used in these instances:

- For future extension of the AMF network. You can pre-configure future AMF network nodes via the **atmf provision node** commands. The following figure illustrates the position of a future, provisioned node. Port1.1.5 on Member 2 and port1.0.3 on Member 4 would need to be configured to expect the future node

Figure 60-19: Provisioning for a future node



- For replacing an existing node with a new node of a **different platform** (e.g. replacing an x310 switch with an x510), and/or with a **different host name**. Using the **atmf provision node** commands you can configure the ports on adjacent nodes to accept a replacement AMF member.

Note If you are replacing an existing node with a new node of the **same platform and host name**, refer to **"Node Recovery" on page 60.31**. In this case, node provisioning is not necessary, and node recovery will suffice.

Creating a new provisioned node

You can pre-configure nodes by **creating** a new directory or by **cloning** an existing node (see **Table 60-7** and **Table 60-8**).

These two methods can briefly be described as:

1. Using the **atmf provision node create** command on page 61.33.

   This command creates an "empty" directory to which release and configuration files can be added for use on a future node. You can copy configuration and release files from existing switches into the new directory. Alternatively, you can create the configuration files by following the instructions in these sections:

   « **"Creating and Using Configuration Files" on page 6.8**

   « **"Configuring AMF" on page 60.13**.

2. Using the **atmf provision node clone** command on page 61.29.

   This command creates a new directory and copies most settings and files from another backup or provisioned node. You can make additional changes manually to these files, if needed.

   We recommend that you select the donor node to be as close as possible to the new node, and for it to contain the same number of ports. This will limit the number of manual changes that will be required to the replicated configuration of the new node.

AMF stores the configuration files for the provisioned node on the master node's backup media or a remote backup server. These files are automatically loaded onto the new node's Flash when it is introduced to the network.

Configuring adjacent nodes

You need to configure the AMF links and cross-links on the adjacent node before the new node is connected. Later, when the provisioned node is introduced to the AMF network, the adjacent node(s) will recognize it and the new node will automatically join the AMF network.

If you plan to **replace** an existing AMF node with one that has a **different host name**, use the **"atmf provision" on page 61.28** to configure the adjacent node to expect the new node in the future. This command is used to configure all AMF links and cross-links to the new node.

If you plan to **extend** your AMF network via ports that have not been used before, you must first fully configure the ports beforehand. Such configuration includes using the **"atmf provision" on page 61.28** and other commands, some of which are shown in the following tables.

More information on configuring switches can be found in **"Creating and Using Configuration Files" on page 6.8**.

Table 60-7 on page 60.44 outlines the procedures to follow if you want to:

- **create** a provisioned node.
- configure the existing node(s) that the provisioned node will eventually connect to.

Table 60-8 on page 60.45 outlines the procedures to follow if you want to:

- **clone** a provisioned node.
- configure the existing node(s) that the provisioned node will eventually connect to.

Note that these examples describe steps for any AMF node, but GS900MX/MPX switches can only be configured as AMF edge switches with a single uplink and no cross-links.

Table 60-7: Procedure for creating a provisioned node and configuring its adjacent node(s)

Step a.	Enter Privileged Exec mode	`Member_4>enable`
Step b.	Set the name of the provisioned node to "future_node"	`Member_4#atmf provision node future_node create` This command sets up an empty directory on the backup media for use with a provisioned node.

Step c.	Copy and set release file	To copy a release file from member4's Flash into the future_node directory, and set that release file to load onto future_node when it first boots up, enter the following commands:
		
		`Member_4#atmf provision node future_node locate`
		`Member_4#copy flash:member4.rel ./future_node.rel`
		`Member_4#atmf provision node future_node configure boot system future_node.rel`
		
		OR
		
		`Member_4#atmf provision node future_node locate`
		`Member_4#copy current-software member4.rel ./future_node.rel`
		`Member_4#atmf provision node future_node configure boot system future_node.rel`
		
		For information on downloading AlliedWare Plus release files see the Download Centre at **www.alliedtelesis.com/support**
		For information on copying files see **"Copying Files to and from Your Device" on page 6.12**

Step d.	Copy and set configuration file	To copy a configuration file named current.cfg from member4's Flash into the future_node directory, and set that configuration file to load onto future_node when it first boots up, enter the following commands:
		
		`Member_4#atmf provision node future_node locate`
		`Member_4#copy flash:current.cfg ./future_node.cfg`
		`Member_4#atmf provision node future_node configure boot config future_node.cfg`
		
		For information on configuring a switch see **"Creating and Using Configuration Files" on page 6.8**
		For information on configuring a switch for AMF see **"Configuring AMF" on page 60.13**

Step e.	Edit configuration file if necessary.	Note that it is important to give the provisioned node a unique hostname. To alter the config file in the AlliedWare Plus text editor, use the **edit** command on page 7.24. For information on configuring a switch see **"Creating and Using Configuration Files" on page 6.8** For information on configuring a switch for AMF see **"Configuring AMF" on page 60.13**

Step f.	Copy and set license file	To copy a license certificate named member_4.txt from member4's Flash into the future_node directory, and set that license certificate to load onto future_node when it first boots up, enter the following commands:
		
		`Member_4#atmf provision node future_node locate`
		`Member_4#copy flash:member_4.txt ./future_node.txt`
		`Member_4#atmf provision node future_node license-cert future_node.txt`
		
		For information on licensing for AMF see the **atmf provision node license-cert** command on page 61.37.

Step g.	Configure the port node(s) that will be connected to the provisioned node. In this example, port1.0.3 on member4 is being configured as an AMF link and to expect the provisioned node future_node	`Member_4#configure terminal`
		`Member_4(config)#interface port1.0.3`
		`Member_4(config-if)#switchport atmf-link`
		`Member_4(config-if)#switchport trunk native vlan none`
		`Member_4(config-if)#atmf provision future_node`
		`Member_4(config-if)#exit`
		`Member_4(config)#exit`
		`Member_4#atmf working-set group local`
		
		Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.
		
		Step g can be repeated to configure the ports on other adjacent nodes that will be connected to the provisioned node.

Table 60-8: Procedure for cloning a provisioned node and configuring its adjacent nodes

Step a.	**Enter Privileged Exec mode**	`AMF_Master1>enable`
Step b.	**Set the name of the provisioned node to "future_node". In this example, the provisioned node will be a clone of member_3**	`AMF_Master1#atmf provision node future_node clone member_3` If further changes are required, follow the commands shown in **Step c** in **Table 60-7** above.

Step c.	**Configure the port node(s) that will be connected to the provisioned node. In this example, port1.0.3 on member_4 is being configured as an AMF link and to expect the provisioned node future_node**	`AMF_Master1#atmf working-set member_4`
		`member_4#configure terminal`
		`member_4(config)#interface port1.0.3`
		`member_4(config-if)#switchport atmf-link`
		`member_4(config-if)#switchport trunk native vlan none`
		`member_4(config-if)#atmf provision future_node`
		`member_4(config-if)#exit`
		`member_4(config)#exit`
		`member_4#atmf working-set group local`
		`AMF_Master1#`
		
		Note that AMF links and crosslinks do not need to be configured with data VLANs and can be used solely to provide AMF management VLAN redundancy.
		
		Step c can be repeated to configure the ports on other adjacent nodes to expect the provisioned node.

Connecting a provisioned node to an AMF network

When you add the new node to the AMF network, its settings and files are automatically downloaded from the master node's backup media, or a remote backup server, to the new node's Flash.

All you need to do is cable the new device into the network. The switch's port LEDs will flash to show that its settings are being loaded. Progressive strobing of all the port LEDs indicates that a recovery is underway. For more information on the node recovery LEDs see **"Recovery progress indication" on page 60.32**.

The following example shows the expected output when a provisioned node named *future_node* joins the AMF network to replace a node called *member_5*.

```
21:57:35 awplus ATMF[999]: ATMF network detected
21:57:35 awplus ATMF[999]: ATMF safe config applied (forwarding disabled)
21:57:45 awplus ATMF[999]: Shutting down all non ATMF ports
21:57:45 awplus ATMF[999]: member_5 has left. 0 member in total.
21:57:45 x510-2 ATMF[999]: future_node has joined. 1 member in total.
21:57:45 x510-2 ATMF[999]: Automatic node recovery started
21:57:45 x510-2 ATMF[999]: Attempting to recover as future_node
21:57:46 x510-2 ATMF[999]: Checking master node availability
21:57:52 x510-2 ATMF[999]: AMF_Master1 has joined. 2 members in total.
21:57:54 x510-2 ATMF[999]: member_1 has joined. 3 members in total.
21:57:56 x510-2 ATMF[999]: member_2 has joined. 4 members in total.
21:58:00 x510-2 ATMF[999]: member_3 has joined. 5 members in total.
21:58:03 x510-2 ATMF[999]: member_4 has joined. 6 members in total.
21:58:04 x510-2 ATMFFSR[6779]: Retrieving recovery data from master node
AMF_Master1
21:58:34 x510-2 ATMFFSR[6779]: Licence installed from certificate.
21:58:35 x510-2 ATMFFSR[6779]: File recovery from master node succeeded. Node will
now reboot
```

Chapter 61: AMF Commands

Introduction 61.3
AMF on GS900MX/MPX Series Switches: AMF Edge 61.3
AMF Naming Convention 61.3
atmf backup 61.4
atmf backup bandwidth 61.5
atmf backup delete 61.6
atmf backup enable 61.7
atmf backup now 61.8
atmf backup server 61.10
atmf backup stop 61.12
atmf backup synchronize 61.13
atmf cleanup 61.14
atmf distribute firmware 61.15
atmf domain vlan 61.17
atmf enable 61.18
atmf group (membership) 61.19
atmf log-verbose 61.21
atmf management subnet 61.22
atmf management vlan 61.24
atmf master 61.26
atmf network-name 61.27
atmf provision 61.28
atmf provision node clone 61.29
atmf provision node configure boot config 61.31
atmf provision node configure boot system 61.32
atmf provision node create 61.33
atmf provision node delete 61.35
atmf provision node license-cert 61.37
atmf provision node locate 61.39
atmf reboot-rolling 61.40
atmf recover 61.44
atmf recover led-off 61.45
atmf remote-login 61.46
atmf restricted-login 61.47
atmf working-set 61.48
clear atmf links statistics 61.49
debug atmf 61.50
debug atmf packet 61.52
erase factory-default 61.55
show atmf 61.56
show atmf backup 61.60
show atmf detail 61.63
show atmf group 61.65
show atmf group members 61.67
show atmf links 61.69
show atmf links detail 61.70
show atmf links statistics 61.76

show atmf memory 61.79
show atmf nodes 61.80
show atmf provision nodes 61.81
show atmf tech 61.82
show atmf working-set 61.84
show debugging atmf 61.85
show debugging atmf packet 61.86
show running-config atmf 61.87
switchport atmf-link 61.88
type atmf node 61.89

Introduction

This chapter provides an alphabetical reference for AMF commands.

AMF on GS900MX/MPX Series Switches: AMF Edge

The GS900MX/MPX Series are edge switches, and can only join the edge of an AMF network.

GS900MX/MPX switches cannot act as AMF master nodes. For completeness, this chapter includes the commands for configuring AMF master nodes, but these commands are not supported on GS900MX/MPX switches.

Each GS900MX/MPX switch can only have a single link to the rest of the AMF network, which must be an uplink to a switch that is closer to the AMF master. They cannot act as intermediate nodes, and they cannot link to other nodes at the same level of the heirarchy as themselves.

This functionality is known as “AMF Edge”.

AMF Naming Convention

When AMF is enabled on a switch, it will automatically be assigned a host name. If a host name has already been assigned, by using the command **“hostname” on page 8.17**, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, **host_** followed (without a space) by the MAC address of the device. For example, a device whose MAC address is **0016.76b1.7a5e** will have the name **host_0016_76b1_7a5e** assigned to it.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network switches, and accordingly apply an appropriate hostname to each switch in your AMF network.

atmf backup

This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

Syntax

```
atmf backup {default|<hh:mm> frequency <1-24>}
no atmf backup enable
```

Parameter	Description
`default`	Restore the default backup schedule.
<hh:mm>	Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock.
`backup`	Enables AMF backup to external media.
`frequency <1-24>`	Sets the number of times within a 24 hour period that backups will be taken.

Default Backups run daily at 03:00 AM, by default

Mode Global Configuration

Usage Running this command only configures the schedule. To enable the schedule, you should then apply the command **atmf backup enable**.

Example To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
VCF_1# configure terminal
VCF_1(config)# atmf backup 11:00 frequency 2
```

Caution File names that comprise identical text, but with differing case, such as Test.txt and test.txt, will not be recognized as being different on a FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based switch. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.

Related Commands

atmf backup enable
atmf backup stop
show atmf backup

atmf backup bandwidth

This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

Note

This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.

Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

Syntax

```
atmf backup bandwidth <0-1000>

no atmf backup bandwidth
```

Parameter	Description
<0-1000>	Sets the bandwidth in kilobytes per second (kBps)

Default The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

Mode Global Configuration

Examples To set an atmf backup bandwidth of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the atmf backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

Related Commands **show atmf backup**

atmf backup delete

This command removes the backup file from the external media of a specified AMF node.

Syntax `atmf backup delete <node-name>`

Parameter	Description
<node-name>	The AMF node name of the backup file to be deleted.

Mode Privileged Exec

Example To delete the backup file from node2, use the following command:

```
Node_1# atmf backup delete node2
```

Related Commands
show atmf backup
atmf backup now
atmf backup stop

atmf backup enable

This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the **atmf backup** command on page 61.4. Note that backups are initiated and stored only on the master nodes.

Use the **no** variant of this command to disable any AMF backups that have been scheduled and previously enabled.

Syntax

```
atmf backup enable

no atmf backup enable
```

Default Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

Mode Global Configuration

Usage A warning message will appear if you run the **atmf backup enable** command with either insufficient or marginal memory availability on your external storage device.

You can use the command **"show atmf backup" on page 61.60** to check the amount of space available on your external storage device.

Example To turn on automatic AMF backup, use the following command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

Related Commands

show atmf
show atmf backup
atmf backup
atmf backup now
atmf enable

atmf backup now

This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the switch on which this command is run, even though the selected AMF member may not be a master node.

Syntax `atmf backup now [<nodename>]`

Parameter	Description
<nodename> or *<hostname>*	The name of the AMF member to be backed up - as set by the command **"hostname" on page 8.17**. Where no name has been assigned to this device, then you must apply the prefix, host underscore followed (without a space) by the MAC address of the device to be backed up. For example `host_0016_76b1_7a5e` Note that the node-name appears as the command Prompt when in Privileged Exec mode.

Default A backup is initiated for all nodes on the AMF (but stored on the master nodes).

Mode Privileged Exec

Usage Although this command will select the AMF node to be backed-up; it can only be run from any AMF master node.

Note The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in **"Example 4" on page 61.9**.

Example 1 In this example, an AMF member has not been assigned a host name. The following command is run on the AMF_Master_2 node to immediately backup the device - identified by its MAC address of 0016.76b1.7a5e:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

Note When a host name is derived from its MAC address, the syntax format entered changes from XXXX.XXXX.XXXX to XXXX_XXXX_XXXX.

Example 2 In this example, an AMF member has the host name, **office_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the switch's master node named **AMF_Master_2** and initiates an immediate backup on the switch named **office_annex**.

Example 3 To initiate from AMF_master_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

Example 4 To initiate an immediate backup of the node with the host-name “office_annex” and store the configuration on both masters, use the following process:

From the AMF_master_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
============================
AMF_Master_1, AMF_Master_2
============================

Working set join
```

Backup the AMF member with the host name, **office_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

Related Commands

atmf backup
atmf backup stop
hostname
show atmf backup

atmf backup server

This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

Syntax

```
atmf backup server id {1|2} <hostlocation> username <username>[path
    <path>|port <1-65535>]

no atmf backup server id {1|2}
```

Parameter	Description
id	Remote server backup server identifier.
{1|2}	The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server.
<hostlocation>	Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).
username	Configure the username to log in with on the selected remote file server.
<username>	The selected remote file server's username.
path	The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.
<path>	The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.
port	The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.
<1-65535>	A TCP port within the specified range.

Defaults Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

Mode Global Exec

Usage The hostname and username parameters must both be configured.

Examples To configure a remote backup server at 192.168.1.1 with the login username of backup1, the backup repository on atmf/network/location/ port 1024, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
                      username backup1 path atmf/network/
                      location/port 1024
```

To configure server 1 with an ipv4 address and a username of backup1, use the commands:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an ipv6 address and a username of backup1, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username
backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2
```

To configure server 2 with a hostname and username in addition, the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

Related Commands **show atmf backup**

atmf backup stop

Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Syntax `atmf backup stop`

Mode Privileged Exec

Usage This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example To stop a backup that is currently executing on master node VCF-1, use the following command:

```
AMF_Master_1# amf backup stop
```

Related Commands
atmf backup
atmf backup enable
atmf backup now
show atmf backup

atmf backup synchronize

For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Syntax `atmf backup synchronize`

Mode Privileged Exec

Example When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

Related Commands
show atmf backup
atmf backup enable
show atmf

atmf cleanup

This command erases all data from NVS and all data from Flash **excluding** the following:

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw_v2.lic

It then reboots to put the device in a clean state ready to be used as a replacement node on a provisioned port.

Syntax `atmf cleanup`

Mode Privileged Exec

Usage This command is an alias to the **erase factory-default** command on page 61.55.

Example To erase data, use the command:

```
Node_1(config)# atmf cleanup

This command will erase all NVS, all flash contents except
for the boot release, and any license files, and then
reboot the switch. Continue? (y/n):y
```

Related Commands **erase factory-default**

atmf distribute firmware

This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash the software release is copied to flash on the new location.

The new release name is updated using the **boot system** command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the **reboot** command should be used on the working-set.

Syntax `atmf distribute firmware <url>`

Parameter	Description
<url>	The URL of the file. See **"URL Syntax" on page 6.12** for valid URL syntax.

Mode Privileged Exec

Examples To upgrade nodes in a atmf network with a predefined AMF group called `sw_team`, use the following commands:

```
SW_Team1# atmf working-set group sw_team
```

Output

```
============================
SW_Team1, SW_Team2, SW_Team3:
============================

Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

Output

```
Retrieving data from SW_Team1
Retrieving data from SW_Team2
Retrieving data from SW_Team3

ATMF Firmware Upgrade:


Node Name          New Release File           Status
-----------------------------------------------------------------
SW_Team1           x510-main-20140204-2.rel   Release ready
SW_Team2           x610-main-20140204-2.rel   Release ready
SW_Team3           x610-main-20140204-2.rel   Release ready
Continue the rolling reboot ? (y/n):y
=================================================================
Copying Release    : x510-main-20140204-2.rel to SW_Team1
Updating Release   : x510-main-20140204-2.rel information on SW_Team1
=================================================================
Copying Release    : x610-main-20140204-2.rel to SW_Team2
Updating Release   : x610-main-20140204-2.rel information on SW_Team2
=================================================================
Copying Release    : x610-main-20140204-2.rel to SW_Team3
Updating Release   : x610-main-20140204-2.rel information on SW_Team3

=================================================================
New firmware will not take effect until nodes are rebooted.
=================================================================

ATMF_NETWORK[3]#
```

Related Commands atmf working-set

atmf domain vlan

The AMF domain vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

When an AMF network is first created all its nodes are assigned a domain VLAN with a default (domain) VID of 4091. An important point conceptually is that although this VLAN then exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANS each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANs are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

If you assign a VLAN ID to this VLAN (i.e. changing its value from the default of 4091) then you will need to do this separately on every device within the AMF network. The AMF domain subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

Syntax

```
atmf domain vlan <2-4090>
no atmf domain vlan .
```

Parameter	Description
<2-4090>	The VLAN number in the range 2 to 4090.

Default The default domain VLAN ID for the AMF is 4091.

Mode Global Configuration

Usage The VLANs involved in this process, must be reserved for AMF and cannot be used for other purposes. This command enables you to change the domain VLAN to match your network's specific configuration.

Caution

Setting this command, then rebooting the switch will only apply the AMF VLAN for the switch being configured. The new domain vlan will not become effective for the AMF network until all its member nodes have been updated, and all its member switches rebooted.

As part of its automatic creation process, this VLAN will also be assigned an IP subnet address based on the value configured by the command **"atmf management subnet" on page 61.22**. Refer to this command for more information.

Examples To change the AMF domain VLAN to 4000 use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# atmf domain vlan 4000
```

To reset the AMF domain VLAN to its default of 4091, use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# no atmf domain vlan
```

atmf enable

This command manually enables (turns on) the AMF feature for the switch being configured.

Use the **no** variant of this command to disable (turn off) the AMF feature on the member node.

Syntax

```
atmf enable
no atmf enable
```

Default Once AMF is configured, the AMF feature starts automatically when the switch starts up.

Mode Global Configuration

Usage The switch does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your switch with any domain specific (non default) settings before enabling AMF.

Examples To turn on the AMF the feature:

```
MyNode# config terminal
MyNode(config)# atmf enable
```

To turn off the AMF feature:

```
MyNode(config)# no atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take
effect.
```

atmf group (membership)

This command configures a switch to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - « all - All nodes in the AMF
  - « current - The current working-set
  - « local - The originating node.

  Note that the Implicit Groups do not appear in show group output.
- Automatic Groups - These are defined by hardware architecture, e.g. x510, x610, x900, x8100.
- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x610, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the **no** variant of this command to remove the membership.

Syntax

```
atmf group <group-list>
no atmf group <group-list>
```

Parameter	Description
<group-list>	A list of group names. These should be entered as a comma delimited list without spaces.

Mode Global Configuration

Usage You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the switch to be members of three groups; two are company departments, and one comprises all devices located in building_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the **atmf group (membership)** command to all members of the working set.

Example To specify the switch to become a member of AMF groups named, Marketing, Sales, and Building_2, use the following command:

```
VCF-1# configure terminal
VCF-1(config)# atmf group marketing,sales,building_2
```

First add the nodes “master_node1” and “member_node_1” to the working-set:

```
master_node# atmf working-set master_node1,member_node_1
```

This command returns the following output confirming that the nodes “master_node” and “node_2” are now part of the working-set:

```
====================
master_node1, member_node_1
======================

Working set join
```

```
atmf-net[2]# configure terminal
```

Add the groups building1 and sales to the working-set

```
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
```

Show the groups that are members of the working-set

```
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
====================
master_node1
======================

AMF group information

building1, sales, master, poe, x8100
```

Related Commands **show atmf group**
show atmf group members

atmf log-verbose

This command limits the number of log messages displayed on the console or permanently logged.

Syntax

```
atmf log-verbose <1-3>
no atmf log-verbose
```

Parameter	Description
<1-3>	The verbose limitation (3 = noisiest, 1 = quietest)

Default The default log display is 3.

Usage This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

Mode Global Configuration

Example To set the log-verbose to noise level 2, use the command:

```
VCF-1# configure terminal
VCF-1(config)# atmf log-verbose 2
```

Validation Command **show atmf**

atmf management subnet

This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section of this command description.

AMF uses these internal IPv4 subnets when exchanging its inter nodal status packets. These subnet addresses must be reserved for AMF and should be used for no other purpose.

The new management subnet will not become effective until all members of the AMF network have been updated and all its units rebooted.

Use the **no** variant of this command to remove the assigned subnet VLANs.

Syntax

```
atmf management subnet <a.b.0.0>

no atmf management subnet
```

Parameter	Description
<a.b.0.0>	The IP address selected for the management subnet. Because a mask of 255.255.0.0 (i.e. /16) will be applied automatically, an IP address in the format a.b.0.0 must be selected. Usually this subnet address is selected from an appropriate range from within the private address space of 172.16.0 to 172.31.255.255, or 192.168.0.0 as defined in RFC1918.

Default 172.31.0.0 (Note that a subnet mask of 255.255.0.0 will automatically be applied).

Mode Global Configuration

Usage Typically a network administrator would use this command to change the default subnet address to match local network requirements.

As previously mentioned, running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the **atmf management vlan**
- 172.31.128.0/17 assigned to the **atmf domain vlan**.

Examples To change the AMF management subnet address on node VCF-1 to 172.25.0.0:

```
VCF-1# configure terminal
VCF-1(config)# atmf management subnet 172.25.0.0
```

To change the AMF management subnet address on node VCF-1 back to its default of 172.31.0.0:

```
VCF-1# configure terminal
VCF-1(config)# no atmf management subnet
```

atmf management vlan

The AMF management VLAN is created when the AMF network is first initiated and is assigned its default VID of 4092. This command enables you to change the VID from this default value.

The AMF management vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (such as the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

If you assign a VLAN ID to this VLAN (i.e. change its value from the default of 4092) then you will need to do this separately on every device within the AMF. The AMF management subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **no** variant of this command to restore the VID to the default of 4092.

Syntax

```
atmf management vlan <2-4090>
no atmf management vlan
```

Parameter	Description
<2-4090>	The VID assigned to the AMF management VLAN.

Default The default VLAN ID for the AMF is 4092.

Note Although the value applied by default lies outside the user configurable range. You can use the "no" form of this command to reset the VLAN to its default value.

Mode Global Configuration

Usage You can use this command to change the management VLAN to meet your network's requirements and standards, particularly in situations where the default address value is unacceptable.

Note This VLAN will automatically be assigned an IP subnet address based on the value configured by the command **"atmf management subnet" on page 61.22**. Refer to this command description for further details.

Examples To change the AMF management VLAN to 4090 use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# atmf management vlan 4090
```

To reset the AMF domain VLAN to its default of 4092, use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# no atmf management vlan
```

Related Commands **atmf domain vlan**
show atmf

atmf master

This command configures the switch to be an AMF master node and automatically creates an AMF master group. The master node is considered to be the core of the AMF network, and must be present for the AMF to form. The AMF master has its node depth set to 0. Note that the node depth vertical distance is determined by the number of uplinks/ downlinks that exist between the node and its master.

An AMF master node must be present for an AMF network to form. Up to two AMF master nodes may exist in a network, and they **must** be connected by an AMF crosslink.

Note Master nodes are an essential component of an AMF network. In order to run AMF, an AMF License is required for each master node.

If the crosslink between two AMF masters fails, then one of the masters will become isolated from the rest of the AMF network.

Use the **no** variant of this command to remove the switch as an AMF master node. The node will retain its node depth of 0 until the network is rebooted.

Note Node depth is the vertical distance (or level) from the master node (whose depth value is 0).

Syntax

```
atmf master
no atmf master
```

Default The switch is not configured to be an AMF master node.

Mode Global Configuration

Example To specify that this node is an AMF master, use the following command:

```
VCF-1# configure terminal
VCF-1(config)# atmf master
```

Related Commands

show atmf
show atmf group

atmf network-name

This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see **"atmf master" on page 61.26**.

Use the **no** variant of this command to remove the AMF network name.

Syntax

```
atmf network-name <name>
no atmf network-name
```

Parameter	Description
<name>	The AMF network name. Up to 15 printable characters can be entered for the network-name.

Mode Global Configuration

Usage This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF. This command will not take effect until the particular node is rebooted.

A switching node (master or member) may be a member of only one AMF network.

Caution

Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).

Example To set the AMF network name to amf_net use the command:

```
Node_1(config)# atmf network-name amf_net
```

atmf provision

This command configures a specified port on an AMF node to accept a provisioned node, via an AMF link, some time in the future.

Use the **no** variant of this command to remove the provisioning on the node.

Syntax

```
atmf provision [<nodename>]
no atmf provision
```

Parameter	Description
<nodename>	The name of the provisioned node that will appear on the AMF network in the future.

Default No provision.

Mode Interface Configuration

Usage The port should be configured as an AMF link or cross link and should be “down” to add or remove a provisioned node.

Example To provision an AMF node named node1 for port1.0.1, use the command:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

Related Commands **switchport atmf-link**
show atmf links

atmf provision node clone

This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command **atmf provision node create**.

Syntax `atmf provision node <nodename> clone <source nodename>`

Parameter	Description
<nodename>	The name that will be assigned to the clone when connected.
<source nodename>	The name of the node whose configuration is to be copied for loading to the clone.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network.

You must run either this command or **atmf provision node create** command, before you can use other "atmf provision node" commands using the specified node name. If a backup or provisioned node already exists for the specified node then you must delete it before using the **atmf provision node** clone command.

When using this command it is important to be aware of the following:

- A copy of *<media>*:atmf/*<atmf_name>*/nodes/*<source_node>*/flash will be made for the provisioned node and stored in the backup media.
- The directory *<node_backup_dir>*/flash/.config/ssh is excluded from the copy.
- All contents of *<root_backup_dir>*/nodes/*<nodename>* will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The "hostname" command is modified to match the name of the provisioned node.
- The "stack virtual-chassis-id" command is removed, if present.

Example To copy from the backup of Switch2 to create backup files for the new provisioned node Switch3 use the following command:

```
switch1# atmf provision node switch3 clone switch2
```

Figure 61-1: Sample output from the atmf provision node clone command

```
switch1#atmf provision node switch3 clone switch2
Copying...
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
switch1# show atmf backup
```

The output from this command is shown in **Figure 61-2**, below, and shows the details of the new provisioned node switch3.

Figure 61-2: Sample output from the show atmf backup command

```
switch1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 ................... Unconfigured
   2 ................... Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
switch3       -            -         No       Yes       Prov
switch1       01 Jan 2014  00:05:49  No       Yes       Good
switch2       01 Jan 2014  00:05:44  Yes      Yes       Good
```

atmf provision node configure boot config

This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the no boot command.

Use the **no** variant of this command to set back to the default.

Syntax

```
atmf provision node <nodename> configure boot config [backup]
   [<file-path|URL>]

atmf provision node [<nodename>] configure no boot config [backup]
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The path or URL and name of the configuration file.

Default No boot configuration files or backup configuration files are specified for the provisioned node.

Mode Privileged Exec

Usage When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the configuration file `branch.cfg` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot
config branch.cfg
```

To set the configuration file `backup.cfg` as the backup to the main configuration file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot
config backup usb:/atmf/amf_net/nodes/node1/
config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config backup
```

Related Commands **atmf provision node configure boot system**
show atmf provision nodes

atmf provision node configure boot system

This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the no boot command.

Use the **no** variant of this command to set back to the default.

This command can only be run on amf master nodes.

Syntax

```
atmf provision node <nodename> configure boot system [backup]
   [<file-path|URL>]

atmf provision node <nodename> configure no boot system [backup]
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The path or URL and name of the release file.

Default No boot release file or backup release files are specified for the provisioned node.

Mode Privileged Exec

Usage When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the release file `x900-5.4.4-1.rel` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot
                system x900-5.4.4-1.rel
```

To set the backup release file `900-5.4.4-1.rel` as the backup to the main release file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot
                system backup card:/atmf/amf_net/nodes/
                node1/flash/x900-5.4.4-1.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
                system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
                system backup
```

Related Commands **atmf provision node configure boot config**
show atmf provision nodes

atmf provision node create

This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing switches. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command **atmf provision node clone**.

This command can only run on amf master nodes.

Syntax `atmf provision node <nodename> create`

Parameter	Description
<nodename>	The name of the node that is being provisioned.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network.

The **atmf provision node create** **atmf** command (or **atmf provision node clone**) must be executed before you can use other "atmf provision node" commands with the specified node name. If a backup or provisioned node already exists for the specified node name then you must delete it before using this command.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

Example To create a new provisioned node named switch2 use the command:

```
switch1# atmf provision node switch2 create
```

Running this command will create the following directories:

- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>
- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>/flash

To confirm the new node's settings, use the command:

```
switch1# show atmf backup
```

The output for the show atmf backup command is shown in **Figure 61-3**, and shows details for the new provisioned node switch2.

Figure 61-3: Sample output from the show atmf backup command

```
switch1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 02 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7315.2MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 ................... Unconfigured
   2 ................... Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
switch2       -            -         No       Yes       Prov
switch1       01 Jan 2014  00:05:49  No       Yes       Good
```

For instructions on how to configure on a provisioned node refer to **"Configuring AMF" on page 60.13** and **"Creating and Using Configuration Files" on page 6.8**.

Related commands **atmf provision node clone**

atmf provision node delete

This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

Syntax `atmf provision node <nodename> delete`

Parameter	Description
<nodename>	The name of the provisioned node to be deleted.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **atmf provision node delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command **atmf backup delete** to delete the files.

Note This command allows provisioned entries to be deleted even if they have been referenced by the **atmf provision** command, so take care to only delete unwanted entries.

Example To delete backup files for a provisioned node named switch3 use the command:

```
switch1# atmf provision node switch3 delete
```

To confirm that the backup files for provisioned node switch3 have been deleted use the command:

```
switch1# show atmf backup
```

The output should show that the provisioned node switch3 no longer exists in the backup file, as shown in **Figure 61-4**:

Figure 61-4: Sample output showing the show atmf backup command

```
switch1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config ......
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 ................... Unconfigured
   2 ................... Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
switch1       01 Jan 2014  00:05:49  No       Yes       Good
switch2       01 Jan 2014  00:05:44  Yes      Yes       Good
```

Related commands atmf provision node create

atmf provision node license-cert

This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on amf master nodes.

Syntax

```
atmf provision node {<nodename>} license-cert <file-path|URL>
no atmf provision node {<nodename>} license-cert
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The name of the certificate file. This can include the file-path of the file.

Default No license certificate file is specified for the provisioned node.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

Example 1 To apply the license certificate cert1.txt stored on tftp server for AMF provisioned node “Switch2”, use the command:

```
switch1# atmf provision node switch2 license-cert
         tftp://192.168.1.1/cert1.txt
```

Example 2 To apply the license certificate cert2.txt stored on AMF master's flash directory for AMF provisioned node “host2”, use the command:

```
switch1# atmf provision node switch2 license-cert/
         cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command **show atmf provision nodes**. The output from this command is shown **Figure 61-5** below, and displays license certification details in the last line.

Figure 61-5: Sample output from the show atmf provision nodes command

```
switch1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                 : switch2
Date & Time               : 06-May-2014 & 23:25:44
Provision Path            : card:/atmf/nodes

Boot configuration :
Current boot image        : x510-1766_atmf_backup.rel (file exists)
Backup  boot image        : x510-main-20140113-2.rel (file exists)
Default boot config       : flash:/default.cfg (file exists)
Current boot config       : flash:/abc.cfg (file exists)
Backup  boot config       : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file           : ./.configs/.sw_v2.lic
                          : ./.configs/.swfeature.lic
Certificate file          : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands show atmf provision nodes

atmf provision node locate

This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on amf master nodes.

Syntax `atmf provision node <nodename> locate`

Parameter	Description
<nodename>	The name of the provisioned node.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network.The command will only work if the provisioned node specified in the command has already been set up. Otherwise, an error message is shown when the command is run.

Note We advise that after running this command, you return to a known working directory, typically flash.

Example To change the working directory that happens to be on switch1 to the directory of provisioned node switch2, use the following command:

```
switch1# atmf provision node switch2 locate
```

The directory of the node switch2 should now be the working directory. You can use the command **pwd** to check this, as shown in the following figure.

Figure 61-6: Sample output from the pwd command

```
switch2#pwd
card:/atmf/building_2/nodes/switch2/flash
```

The output above shows that the working directory is now the flash of switch2.

Related commands **atmf provision node create**
atmf provision node clone
pwd

atmf reboot-rolling

This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the url parameter, you can also upgrade your switches' software one AMF node at a time.

The force command enforces a node reboot even if a previous node does not rejoin the AMF network. In this situation the unsuitable node will time-out and the rolling reboot process stops. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

Syntax `atmf reboot-rolling [force] [<url>]`

Parameter	Description
`force`	Ignore a failed node and move on to the next node. Where a node fails to reboot a timeout is applied based on the time taken during the last reboot.
<url>	The url path to the software upgrade file.

Mode Privileged Exec

Usage You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected location - based on the parameters and URL you have entered.

For example card:/5.4.3/x*-5.4.3-*.rel will select from the folder card:/5.4.3 the latest file that matches the selection x (wildcard) -5.4.3-(wildcard).rel. Because x* is applied, each switch type will be detected and its appropriate release file will be installed.

Other allowable entries are:

- card:*.rel:
  Used when loading SW from SD cards.
- tftp:ip address:
  Used when loading SW from a TFTP server.
- usb:
  Used when loading SW from a USB flash drive.
- flash:
  Used when loading SW from flash memory, i.e. from one x900 switch to another.
- scp:
  Used when loading SW from a secure copy.
- http:
  Used when loading SW from an HTTP file server site.

Several checks are performed to ensure the upgrade will succeed. These include checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash to a new location on each node as it is processed. The new release name will be updated using the "boot system *<release-name>*" command, and the old release will become the backup release file.

Note If you are using TFTP or HTTP, for example, to access a file on a remote device then the URL should specify the exact release filename without using wild card characters.

On bootup the software release is verified. Should an upgrade fail, the upgrading unit will revert back to its previous software version. At the completion of this command, a report is run showing the release upgrade status of each node.

Note Take care when removing external media or rebooting your switches. Removing an external media while files are being written entails a significant risk of causing a file corruption.

Example 1 To reboot all x510 nodes in an AMF network, use the following command:

```
Bld2_Floor_1# atmf working-set group x510
```

This command returns the following type of screen output:

```
==================
node1, node2, node3:
====================

Working set join

AMF_NETWORK_Name[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x510

============================
SW_Team1, SW_Team2, SW_Team3:
============================

Working set join


ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

                     Timeout
Node Name            (Minutes)
--------------------------
SW_Team1                14
SW_Team2                 8
SW_Team3                 8
Continue the rolling reboot ? (y/n):y
================================================
ATMF Rolling Reboot: Rebooting SW_Team1
================================================

% SW_Team1 has left the working-set
Reboot of SW_Team1 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team2
================================================

% SW_Team2 has left the working-set
Reboot of SW_Team2 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team3
================================================

% SW_Team3 has left the working-set
Reboot of SW_Team3 has completed

================================================
ATMF Rolling Reboot Complete
Node Name           Reboot Status
---------------------------------
SW_Team1               Rebooted
SW_Team2               Rebooted
SW_Team3               Rebooted
================================================
```

Example 2 To update firmware releases, use the following command:

```
Node_1# atmf working-set group all
ATMF_NETWORK[9]# atmf reboot-rolling card:/5.4.3/x*-5.4.3-*.rel
```

.

```
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)    New Release File             Status
-------------------------------------------------------------------
SW_Team1               8         x510-5.4.3-0.5.rel           Release Ready
SW_Team2              10         x510-5.4.3-0.5.rel           Release Ready
SW_Team3               8         ---                          Not Supported
HW_Team1               6         ---                          Incompatible
Bld2_Floor_1           6         x900-5.4.3-0.5.rel           Release Ready
Bld1_Floor_2           2         x610-5.4.3-0.5.rel           Release Ready
Bld1_Floor_1           4         ---                          Incompatible
Building_1             2         ---                          Incompatible
Building_2             2         x900-5.4.3-0.5.rel           Release Ready
Continue upgrading releases ? (y/n):
```

atmf recover

This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced. The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. The configuration file of the device being replaced is selected by the nodename parameter, and the master node holding the configuration file is specified by the parameter <*master-nodename*>.

If the <*nodename*> parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used nodename), then the recovery will fail.

If the <*master-nodename*> parameter is not specified then the device will poll all known AMF masters and execute an election process (based on the last successful backup and its timestamp) to determine which master node to use. If no valid backup master is found, then this command will fail.

Syntax `atmf recover [<nodename> <master-nodename>]`

Parameter	Description
`<nodename>`	The name of the device whose configuration is to be recovered or replicated.
`<master-nodename>`	The name of the master device that holds the required configuration information. Note that although you can omit both the nodename and the master nodename; you can only omit the master nodename if you also omit the nodename.

Mode Privileged Exec

Usage No error checking occurs when this command is run, and regardless of the last backup status, the recovering node will attempt to load its configuration from the master node specified by the master-nodename parameter.

Note that if the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.

Example To recover the AMF node named Node_10 from the AMF master node named Master_2, use the following command:

```
Master_2# atmf recover Node_10 Master_2
```

Related Commands
atmf backup stop
show atmf backup
show atmf

atmf recover led-off

This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more detailed information see **"Recovery progress indication" on page 60.32**.

Syntax `atmf recover led-off`

Default Normal operational mode

Mode Privileged Exec

Example To revert the LEDs on Node1 from recovery mode display, to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

Related Commands **atmf recover**

atmf remote-login

Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

Syntax `atmf remote-login [user <name>] <nodename>`

Parameter	Description
<name>	User name.
<nodename>	Node name.

Mode Privileged Exec (This command will only run at privilege level 15)

Usage You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (i.e. device reboot) you will be returned to the originating node.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

Example 1 To remotely login from node Node10 to Node20 use the following command:

```
Node10# atmf remote-login node20
```

Example 2 In this example, user Whitney is a valid user of node5. She can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user whitney
       node3
Type 'exit' to return to node5#

node3> enable
```

Note In the above example the user name whitney is valid on both nodes.

Therefore, to prevent unauthorized access, user names should be unique across all nodes within the AMF network.

atmf restricted-login

This command restricts the use of the **"atmf working-set" on page 61.48** command on all AMF master nodes to privilege 15 users only. Once entered on any AMF master node, this command will propagate across the network.

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

Syntax

```
atmf restricted-login

no atmf restricted-login
```

Mode Privileged Exec

Default Master nodes operate with **atmf restricted-login** disabled.

Member nodes operate with **atmf restricted-login** enabled.

Note

The default conditions of this command vary from those applied by its "no" variant. This is because the restricted-login action is only applied by **master** nodes, and in the absence of a master node, the default is to apply the restricted action to all **member** nodes with AMF configured.

In the presence of a **master** node, its default of "atmf restricted-login disabled" will permeate to all its member nodes. Similarly, any change in this command's status that is made on a master node, will also permeate to all its member nodes

Example To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

Validation Command **show atmf**

atmf working-set

The AMF working-set command enables you to execute commands across an individually listed set (or preselected group) of AMF nodes. Group selection is made using the **atmf group (membership)** command on page 61.19.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - « all - All nodes in the AMF
  - « current - All nodes that comprise the current working-set
  - « local - The originating node.
- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x900, x8100, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in show group output.

If a node is an AMF master it will be automatically added to the master group.

Syntax `atmf working-set {[<node-list>][group{<group-list>|all|local|current}]}`

Parameter	Description
<node-list>	A comma delimited list (without spaces) of nodes to be included in the working-set.
`group`	The AMF group.
<group-list>	A comma delimited list (without spaces) of groups to be included in the working-set. Note that this can include either defined groups, or any of the Automatic, or Implicit Groups shown earlier in the bulleted list of groups.
`all`	All nodes in the AMF.
`local`	Local node Running this command with the parameters **group local** will return you to the local prompt and local node connectivity.
`current`	Nodes in current list.

Default Needs to be entered

Mode Privileged Exec

Example 1 To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf working-set group all
```

Note This command adds the implicit group “all” to the working set, where “all” comprises all nodes in the AMF.

This command displays an output screen similar to the one shown below:

```
=========================================
node1, node2, node3, node4, node5, node6:
=========================================

Working set join

ATMF_NETWORK_Name[6]#
```

Example 2 To return to the local prompt, and connectivity to only the local node; use the command:

```
ATMF_NETWORK_Name[6]# atmf working-set group local

                    node1#
```

Parameter	Description
node1, node2	The name of the nodes - as set by the **hostname** command on page 8.17.
ATMF_Network_Name	The name of the AMF network - as set by the **atmf network-name** command on page 61.27.
[6]	The number of nodes in the working-set.

clear atmf links statistics

This command resets the values of all AMF link, port, and global statistics to zero.

Syntax `clear atmf links statistics`

Mode Privilege Exec

Example To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

Related Commands **show atmf links statistics**

debug atmf

This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The "no" variant of this command disables either all AMF debugging information, or only the particular information as selected by the command's parameters.

Syntax

```
debug atmf [link|crosslink|database|neighbor|error|all]
no debug atmf [link|crosslink|database|neighbor|error|all]
```

Parameter	Description
`link`	Output displays debugging information relating to uplink or downlink information.
`crosslink`	Output displays all crosslink events.
`database`	Output displays only notable database events.
`neighbor`	Output displays only notable AMF neighbor events.
`error`	Output displays AMF error events.
`all`	Output displays all AMF events.

Default All debugging facilities are disabled.

Mode User Exec and Global Configuration

Usage If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

Note An alias to the no variant of this command is **"undebug atmf" on page 61.92**.

Examples To debug all AMF debugging, use the command:

```
node_1# debug atmf
```

To debug all AMF link debugging, use the command:

```
node_1# debug atmf link
```

To debug all AMF crosslink debugging, use the command:

```
node_1# debug atmf crosslink
```

To debug all AMF database debugging, use the command:

```
node_1# debug atmf database
```

To debug all AMF neighbor debugging, use the command:

```
node_1# debug atmf neighbor
```

To debug all AMF error debugging, use the command:

```
node_1# debug atmf error
```

To debug all AMF facilities, use the command:

```
node_1# debug atmf all
```

Related Commands **no debug all**

debug atmf packet

This command configures AMF Packet debugging parameters. The debug only displays information relevant to the current node. The command has following parameters:

Syntax

```
debug atmf packet[[direction {rx|tx|both}][level {1|2|3}][timeout
    <seconds>][num-pkts <quantity>][filter node <name> ][interface
    <ifname>][pkt-type {[1][2][3][4][5][6][7][8][9][10][11]]]
```

Simplified Syntax

debug atmf packet		[direction {rx|tx|both}]
		[level {[1][2|3}]
		[timeout <*seconds*>]
		[num-pkts <*quantity*>]
debug atmf packet	filter	[node <*name*>]
		[interface <*ifname*>]
		[pkt-type [1][2][3][4][5][6][7][8][9][10][11]]

Note You can combine the syntax components shown, but when doing so, you must retain their original order.

Default Level 1, both Tx and Rx, a timeout of 60 seconds with no filters applied.

Note An alias to the no variant of this command - **undebug atmf** - can be found elsewhere in this chapter.

Mode User Exec and Global Configuration

Usage If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

Parameter	Description
direction	Sets debug to packet received, transmitted, or both
rx	packets received by this node
tx	Packets sent from this node
1	AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level.
2	AMF Detailed Packet Information. Enter 2 to select this level.
3	AMF Packet HEX dump. Enter 3 to select this level.
timeout	Sets the execution timeout for packet logging
<seconds>	Seconds
num-pkts	Sets the number of packets to be dumped

Parameter	Description
`pkts`	The actual number of packets
`filter`	Sets debug to filter packets
`node`	Sets the filter on packets for a particular Node
<name>	The name of the remote node
`interface`	Sets the filter to dump packets from an interface (portx.x.x) on the local node
`ifname`	Interface port or virtual-link
`pkt-type`	Sets the filter on packets with a particular AMF packet type
1	Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type.
2	Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type.
3	Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.
4	Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.
5	Non broadcast hello unicast packets. Enter 5 to select this packet type.
6	Stack hello unicast packets. Enter 6 to select this packet type.
7	Database description. Enter 7 to select this packet type.
8	DBE request. Enter 8 to select this packet type.
9	DBE update. Enter 9 to select this packet type.
10	DBE bitmap update. Enter 10 to select this packet type.
11	DBE acknowledgment. Enter 11 to select this packet type.

Examples To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter
node_1
```

To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface
vlink1 pkt-type 1 7 11
```

This example applies the debug atmf packet command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts
60 filter node x900 interface port1.0.1 pkt-
type 4 7 10
```

erase factory-default

This command erases all data from NVS and all data from flash **excluding** the following:

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw_v2.lic

The device is then rebooted and returns the switch to its factory default condition. The switch can then be used for automatic node recovery.

Syntax `erase factory-default`

Mode Global Configuration.

Usage This command is an alias to the **atmf cleanup** command on page 61.14.

Example To erase data, use the command:

```
Node_1(config)# erase factory-default

This command will erase all NVS, all flash contents except
for the boot release, and any license files, and then
reboot the switch. Continue? (y/n):y
```

Related Commands **atmf cleanup**

show atmf

Displays information about the current AMF node.

Syntax `show atmf [summary|tech|nodes|session]`

Parameter	Description
`summary`	Displays summary information about the current AMF node.
`tech`	Displays global AMF information.
`nodes`	Displays a list of AMF nodes together with brief details.
`session`	Displays information on an AMF session.

Default Only summary information is displayed.

Mode User Exec and Privileged Exec

Usage AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes

Example 1 To show summary information on AMF node_1 use the following command:

```
node_1 show atmf summary
```

The following figure shows some example output from running this command for a specific AMF node.

Figure 61-7: Output from the show atmf summary command

```
node_1#show atmf
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : ATMF_NET
Node Name              : node_1
Role                   : Master
Current ATMF Nodes     : 8
```

Example 2 To show information specific to AMF nodes use the following command:

```
node_1 show atmf nodes
```

Figure 61-8: Output from the show atmf nodes command

```
Node Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone

  Node                Device             AMF                              Node
  Name                Type               Master  SC  Parent                Depth
-------------------------------------------------------------------------------
  Building_1          AT-SBx8112           Y     C   -                      0
* Building_2          x900-12XT/S          Y     N   -                      0
  Bld1_Floor_1        SwitchBlade x908     N     S   Building_1             1
  Bld1_Floor_2        x600-24Ts/XP         N     N   Building_1             1
  Bld2_Floor_1        x610-24Ts-POE+       N     N   Building_1             1
  SW_Team1            x510-28GPX           N     N   Bld1_Floor_2           2

 Current AMF node count 8
```

The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session. For example, in the case below, node_1 and node5 have active users logged in.

Example 3 To display AMF active sessions, use the following command:

```
node_1 show atmf session
```

Figure 61-9: Output from the show atmf session command

```
node_1#show atmf session

CLI Session Neighbors

Session ID                            : 73518
Node Name                             : node_1
PID                                   : 7982
Link type                             : Broadcast-cli
MAC Address                           : 0000.0000.0000
Options                               : 0
Our bits                              : 0
Link State                            : Full
Domain Controller                     : 0
Backup Domain Controller              : 0
Database Description Sequence Number  : 00000000
First Adjacency                       : 1
Number Events                         : 0
DBE Retransmit Queue Length           : 0
DBE Request List Length               : 0

Session ID                            : 410804
Node Name                             : node5
PID                                   : 17588
Link type                             : Broadcast-cli
MAC Address                           : 001a.eb56.9020
Options                               : 0
Our bits                              : 0
Link State                            : Full
Domain Controller                     : 0
Backup Domain Controller              : 0
Database Description Sequence Number  : 00000000
First Adjacency                       : 1
Number Events                         : 0
DBE Retransmit Queue Length           : 0
DBE Request List Length               : 0
```

The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

Example 4 To display AMF technical information, use the following command:

```
node_1 show atmf tech
```

Figure 61-10: Output from the show atmf tech command

```
node_1#show atmf tech
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : ATMF_NET
Node Name              : node_1
Role                   : Master
Current ATMF Nodes     : 8

ATMF Technical information:

Network Name                         : ATMF_NET
Domain                               : node_1's domain
Node Depth                           : 0
Domain Flags                         : 0
Authentication Type                  : 0
MAC Address                          : 0014.2299.137d
Board ID                             : 287
Domain State                         : DomainController
Domain Controller                    : node_1
Backup Domain Controller             : node2
Domain controller MAC                : 0014.2299.137d
Parent Domain                        : -
Parent Domain Controller             : -
Parent Domain Controller MAC         : 0000.0000.0000
Number of Domain Events              : 0
Crosslink Ports Blocking             : 0
Uplink Ports Waiting on Sync         : 0
Crosslink Sequence Number            : 7
Domains Sequence Number              : 28
Uplink Sequence Number               : 2
Number of Crosslink Ports            : 1
Number of Domain Nodes               : 2
Number of Neighbors                  : 5
Number of Non Broadcast Neighbors    : 3
Number of Link State Entries         : 1
Number of Up Uplinks                 : 0
Number of Up Uplinks on This Node    : 0
DBE Checksum                         : 84fc6
Number of DBE Entries                : 0
Management Domain Ifindex            : 4391
Management Domain VLAN               : 4091
Management ifindex                   : 4392
Management VLAN                      : 4092
```

Table 61-1: Parameter definitions from the show atmf tech command

Parameter	Definition
ATMF Status	The Node's AMF status, either Enabled or Disabled.
Network Name	The AMF network that a particular node belongs to.
Node Name	The name assigned to a particular node.
Role	The role configured for this AMF device, either Master or Member.
Current ATMF Nodes	The count of AMF nodes in an AMF Network.
Node Address	An Address used to access a remotely located node (.atmf).

Table 61-1: Parameter definitions from the show atmf tech command (cont.)

Parameter	Definition
Node ID	A Unique identifier assigned to a Node on an AMF network.
Node Depth	The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
Domain State	The state of Node in a Domain in AMF network as Controller/Backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between Nodes of different domain (up/down links). ■ VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. ■ Management Subnet - Network prefix for the subnet. ■ Management IP Address - The IP address allocated for this traffic. ■ Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). ■ VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. ■ Domain Subnet. The subnet address used for this traffic. ■ Domain IP Address. The IP address allocated for this traffic. ■ Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
Device Type	The Product Series Name.
ATMF Master	The 'Y' if the node belongs to a Core domain.
SC	The Switch Configuration, C - Chassis(SBx81series), S - Stackable (VCS) and N - Standalone.
Parent	The a Node to which the current node has an active uplink.
Node Depth	The the number of nodes in path from this node to the Core domain.

Related Commands **show atmf detail**

Note

You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

show atmf backup

This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master nodes.

Syntax `show atmf backup [logs|server-status|synchronize [logs]]`

Parameter	Description
`logs`	Displays detailed log information.
`server-status`	Displays connectivity diagnostics information for each configured remote file server.
`synchronize`	Display the file server synchronization status
`logs`	For each remote file server, display the logs for the last synchronization

Mode Privileged Exec

Example 1 To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

```
Node_1# show atmf backup
ScheduledBackup ......Enabled
  Schedule.............1 per day starting at 03:00
  Next Backup Time....19 May 2012 03:00
Backup Media..........SD (Total 1974.0 MB, Free197.6MB)
Current Action........Starting manual backup
Started...............18 May 2012 10:08
CurrentNode...........atmf_testbox1

Node Name                          Date         Time      In ATMF     Status
-------------------------------------------------------------------------------
atmf_testbox1                       17May  2014  09:58:59  Yes         Errors
atmf_testbox2                       17May  2014  10:01:23  Yes         Good

Node_1#show atmf backup logs

Log File Location: card:/atmf/office/logs/rsync_<nodename>.log

Node
Name Log Details-------------------------------------------------------------------
atmf_testbox2
      2014/05/22 03:41:32 [30299]File list size: 6199
      2014/05/22 03:41:32 [30299]File list generation time: 0.011 seconds
      2014/05/22 03:41:32 [30299]File list transfer time: 0.000 seconds
      2014/05/22 03:41:32 [30299]Total bytes sent: 696
      2014/05/22 03:41:32 [30299]Total bytes received: 16.03K
      2014/02/20 03:41:32 [30299]sent 696 bytes rece ived 16.03Kbytes 33.45 K
      bytes/sec
      2014/05/22 03:41:32 [30299]total size is 21.73M speedup is 1298.93
      2014/05/22 03:41:32 [30297]sent 626 bytes received 6203 bytes total
      size 43451648
```

Example 2 To display the AMF backup information with the optional parameter `server-status`, use the command:

```
Node_1# show atmf backup server-status
```

```
Node1#sh atmf backup server-status

Id  Last Check  State
-------------------------------------
1       186 s  File server ready
2           1 s  SSH no route to host
```

Table 61-2: Parameter definitions from the show atmf backup server-status command

Parameter	Definition
`Scheduled Backup`	Indicates whether AMF backup scheduling is enabled or disabled.
`Schedule`	Displays the configured backup schedule.
`Next Backup Time`	Displays the date and time of the next scheduled.
`Backup Media`	The current backup medium in use. This will be one of USB, SD, or NONE. Note that the USB will take precedence over the SD card. Utilized and available memory (MB) will be indicated if backup media memory is present.
`Current Action`	The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).
`Started`	The date and time that the currently executing task was initiated in the format DD MMM YYYY.
`Current Node`	The name of the node that is currently being backed up.
`Node Name`	The name of the node that is storing backup data - on its backup media.
`Date`	The data of the last backup in the format DD MMM YYYY.
`Time`	The time of the last backup in the format HH:MM:SS.
`In ATMF`	Whether the node shown is active in the AMF network, (Yes or No).
`Status`	The output can contain one of four values: ■ "-" meaning that the status file cannot be found or cannot be read. ■ "Errors" meaning that there are issues - note that the backup may still be deemed successful depending on the errors. ■ "Stopped" meaning that the backup attempt was manually aborted;. ■ "Good" meaning that the backup was completed successfully.
`Log File Location`	All backup attempts will generate a result log file in the identified directory based on the node name. In the above example this would be: card:/amf/office/logs/rsync_amf_testbox1.log.
`Log Details`	The contents of the backup log file.
`server-status`	Displays connectivity diagnostics information for each configured remove file server.

Note You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

Related Commands **show atmf**
atmf network-name

show atmf detail

This command displays details about an AMF node. It can only be run on AMF master nodes.

Syntax `show atmf [detail]`

Parameter	Description
`detail`	Displays output in greater depth.

Mode Privileged Exec

Example 1 To display the AMF node1 information in detail, use the command:

```
node1# show atmf detail
```

A typical output screen from this command is shown below:

```
node1#show atmf detail
ATMF Detail Information

Network Name                        : ATMF_NET
Node Name                           : Admin2
Node Address                        : Admin2.atmf
Node ID                             : 15
Node Depth                          : 0
Domain State                        : DomainController
Recovery State                      : None

Management VLAN
 VLAN ID                            : 4092
 Management Subnet                  : 172.31.0.0
 Management IP Address              : 172.31.0.1
 Management Mask                    : 255.255.128.0

Domain VLAN
 VLAN ID                            : 4091
 Domain Subnet                      : 172.31.128.0
 Domain IP Address                  : 172.31.128.1
 Domain Mask                        : 255.255.128.0
```

Table 61-3: Parameter definitions from the show atmf details command

Parameter	Definition
`ATMF Status`	The Node's AMF status, either Enabled or Disabled.
`Network Name`	The AMF network that a particular node belongs to.
`Node Name`	The name assigned to a particular node.
`Role`	The role configured for this AMF device, either Master or Member.
`Current ATMF Nodes`	The count of AMF nodes in an AMF Network.
`Node Address`	An Address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).
`Node ID`	A Unique identifier assigned to a Node on an AMF network.

Table 61-3: Parameter definitions from the show atmf details command (cont.)

Parameter	Definition
`Node Depth`	The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
`Domain State`	The state of Node in a Domain in AMF network as Controller/Backup.
`Recovery State`	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
`Management VLAN`	The VLAN created for traffic between Nodes of different domain (up/down links). ■ VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. ■ Management Subnet - Network prefix for the subnet. ■ Management IP Address - The IP address allocated for this traffic. ■ Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
`Domain VLAN`	The VLAN assigned for traffic between Nodes of same domain (crosslink). ■ VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. ■ Domain Subnet. The subnet address used for this traffic. ■ Domain IP Address. The IP address allocated for this traffic. ■ Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
`Device Type`	The Product Series Name.
`ATMF Master`	'Y' if the node belongs to a Core domain.
`SC`	The Switch Configuration, C - Chassis(SBx81series), S - Stackable (VCS) and N - Standalone.
`Parent`	The a Node to which the current node has an active uplink.
`Node Depth`	The number of nodes in the path from this node to the Core domain.

show atmf group

This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

Syntax `show atmf group [user-defined|automatic]`

Parameter	Description
`user-defined`	User-defined-group information display.
`automatic`	Automatic group information display.

Default All groups are displayed

Mode Privileged Exec

Example 1 To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information
master, x510
node2#
```

This screen shows that node2 contains the groups, master and x510. Note that although the node also contains the implicit groups, these do not appear in the show output.

Example 2 The following commands (entered on node2) will display all the automatic groups within the working set containing node-1 and all nodes that have been pre-defined to contain the sysadmin group:

First define the working-set:

```
Node-1# #atmf working-set node-1 group sysadmin
```

A typical output screen from this command is shown below:

```
ATMF group information

master, poe, x8100


================================================
node-1, node-2, node-3, node-4, node-5, node-6:
================================================

ATMF group information

sysadmin, x8100

ATMF-Test-NETWORK[6]#
```

This confirms that the six nodes (node-1 to node-6) are now members of the working-set and that these nodes reside within the AMF-Test-Network.

Note that to run this command, you must have previously entered the command **"atmf working-set" on page 61.48**. This can be seen from the network level prompt, which in this case is, ATM_Network{6}#.

Figure 61-11: Sample output from the show atmf group command for a working set.

```
ATMF_NETWORK[6]#show atmf group
==============================
node-3, node-4, node-5, node-6:
==============================

ATMF group information

edge_switches, x510
```

Table 61-4: Parameter definitions from the show atmf group command for a working set

Parameter	Definition
`ATMF group information`	Displays a list of nodes and the groups that they belong to, for example: ■ master - Shows a common group name for Nodes configured as AMF masters. ■ Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x900, x610, for example. ■ User-defined - Arbitrary groups created by the user for AMF nodes.

show atmf group members

This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group. User can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

Syntax `show atmf group members [user-defined|automatic]`

Parameter	Description
`user-defined`	User defined group membership display.
`automatic`	Automatic group membership display.

Mode Privileged Exec

Example To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

Figure 61-12: Sample output from the show atmf group members command

```
ATMF Group membership


Automatic         Total
Groups            Members   Members
------------------------------------------------------------------
master            1         Building_1
poe               1         HW_Team1
x510              3         SW_Team1 SW_Team2 SW_Team3
x900              1         Bld1_Floor_2
x610              1         HW_Team1
x8100             2         Building_1 Building_2


ATMF Group membership

User-defined      Total
Groups            Members   Members
------------------------------------------------------------------
marketing           1       Bld1_Floor_1
software            3       SW_Team1 SW_Team2 SW_Team3
```

Table 61-5: Parameter definitions from the show atmf group members command

Parameter	Definition
`Automatic Groups`	Lists the Automatic Groups and their nodal composition. The sample output shows AMF nodes based on same Hardware type or belonging to same Master group.
`User-defined Groups`	Shows grouping of AMF nodes in user defined groups.
`Total Members`	Shows the total number of members in each group.
`Members`	Shows the list of AMF Nodes in each group.

Related Commands **show atmf group**
show atmf
atmf group (membership)

show atmf links

This command displays brief information about AMF links on a switch, such as link status and adjacent nodes.

Provisioned node names will be displayed with a trailing * character, and will not have an entry under Adjacent Ifindex.

This command can only be run on AMF master nodes.

Syntax `show atmf links`

Mode User Exec and Privileged Exec

Example To display the AMF links brief details, use the following command:

```
switch1# show atmf links brief
```

Related Commands
no debug all
clear atmf links statistics
show atmf
show atmf nodes

show atmf links detail

This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master nodes.

Syntax `show atmf links [detail]`

Parameter	Description
`detail`	Detailed AMF links information.

Mode User Exec

Example To display the AMF link details use this command:

```
switch1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links.

Figure 61-13: Sample output from the show atmf links detail command

```
switch1# show atmf links details

ATMF  Links Detail:

Port                                : sa1
Ifindex                             : 4501
VR ID                               : 0
Port Status                         : Up
Port State                          : Full
Port BPDU Receive Count             : 44441
Adjacent Node Name                  : Building_2
Adjacent Ifindex                    : 4501
Adjacent VR ID                      : 0
Adjacent MAC                        : 0014.2299.137d
Port Last Message Response          : 0
```

Figure 61-13: Sample output from the show atmf links detail command (cont.)

```
Port                                  : port2.0.2
Ifindex                               : 6002
VR ID                                 : 0
Port Status                           : Down
Port State                            : Init
Port BPDU Receive Count               : 0

Link State Entries:

Node.Ifindex                          : Building_2.4501 -
Building_1.4501
Transaction ID                        : 3 - 3
MAC Address                           : 0014.2299.137d -
eccd.6d03.10e3
Link State                            : Full - Full

Domain Nodes Tree:

Node                                  : Building_2
  Links on Node                       : 1
  Link 0                              : Building_2.4501 -
Building_1.4501
  Forwarding State                    : Forwarding
Node                                  : Building_1
  Links on Node                       : 1
  Link 0                              : Building_2.4501 -
Building_1.4501
  Forwarding State                    : Forwarding
```

```
Crosslink Transaction Entries:

Node                                  : Building_2
Transaction ID                        : 3
Uplink Transaction ID                 : 3
Uplink Information:

Waiting for Sync                      : 0
Transaction ID                        : 3
Number of Links                       : 0
Number of Local Uplinks               : 0
```

```
Uplink Information:

Waiting for Sync                      : 0
Transaction ID                        : 3
Number of Links                       : 0
Number of Local Uplinks               : 0

Originating Node                      : Building_2
Domain                                : -'s domain
Node                                  : Building_2
Ifindex                               : 0
VR ID                                 : 0
Transaction ID                        : 3
Flags                                 : 32
Domain Controller                     : -
Domain Controller MAC                 : 0000.0000.0000
```

Figure 61-13: Sample output from the show atmf links detail command (cont.)

```
Downlink Domain Information:

Domain                                : Bld2_Floor_1's domain
  Domain Controller                   : Bld2_Floor_1
  Domain Controller MAC               : eccd.6d3f.fef7
  Number of Links                     : 2
  Number of Links Up                  : 2
  Number of Links on This Node        : 1
  Links are Blocked                   : 0
  Node Transaction List
    Node                              : Building_2
    Transaction ID                    : 7
  Domain List
    Domain                            : Bld2_Floor_1's domain
      Node                            : Building_2
      Ifindex                         : 5002
      Transaction ID                  : 7
      Flags                           : 1

    Domain                            : Bld2_Floor_1's domain
      Node                            : Building_1
      Ifindex                         : 7002
      Transaction ID                  : 7
      Flags                           : 1
```

```
------------------------------------------------------------------
Up/Downlink Ports Information
------------------------------------------------------------------
Port                                  : port1.3.1
Ifindex                               : 7001
VR ID                                 : 0
Port Status                           : Up
Port State                            : Full
Adjacent Node                         : Bld1_Floor_1
Adjacent Internal ID                  : 4
Adjacent Ifindex                      : 6001
Adjacent Board ID                     : 290
Adjacent VR ID                        : 0
Adjacent MAC                          : 0000.cd37.0ea4
Adjacent Domain Controller            : Bld1_Floor_1
Adjacent Domain Controller MAC        : 0000.cd37.0ea4
Port Forwarding State                 : Blocking
Port BPDU Receive Count               : 0
Port Sequence Number                  : 12
Port Adjacent Sequence Number         : 9
Port Last Message Response            : 0
```

```
Port                                  : port1.3.2
Ifindex                               : 7002
VR ID                                 : 0
Port Status                           : Up
Port State                            : Full
Adjacent Node                         : Bld2_Floor_1
Adjacent Internal ID                  : 3
Adjacent Ifindex                      : 5001
Adjacent Board ID                     : 333
Adjacent VR ID                        : 0
Adjacent MAC                          : eccd.6d3f.fef7
Adjacent Domain Controller            : Bld2_Floor_1
Adjacent Domain Controller MAC        : eccd.6d3f.fef7
Port Forwarding State                 : Blocking
Port BPDU Receive Count               : 0
Port Sequence Number                  : 15
Port Adjacent Sequence Number         : 8
Port Last Message Response            : 0
```

Table 61-6: Parameter definitions from the show atmf links detail command output

Parameter	Definition
`Port Status`	Shows status of the local port on the Node as UP/DOWN.
`Adjacent Node`	Shows Adjacent AMF Node to this Node.
`Adjacent IfIndex`	Shows interface on the Adjacent AMF Node connected to this Node.
`Link State`	Shows state of AMF link Forwarding/Blocking.
`Crosslink Ports Information`	Show details of all Crosslink ports on this Node: ■ Port - Name of the Port or static aggregation (sa<*>). ■ Ifindex - Interface index for the crosslink port. ■ VR ID - Virtual router id for the crosslink port. ■ Port Status - Shows status of the local port on the Node as UP/DOWN. ■ Port State - Same as AMF state as described above. ■ Port BPDU Receive Count - The number of AMF protocol PDU's received. ■ Adjacent Node Name - name of the adjacent node in the domain. ■ Adjacent Ifindex - Ifindex of the adjacent node in the domain. ■ Adjacent VR ID - Virtual router id of the adjacent node in the domain. ■ Adjacent MAC - MAC address of the adjacent node in the domain. ■ Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.
`Link State Entries`	Show all the link state database entries: ■ Node.Ifindex - Shows adjacent Node names and Interface index. ■ Transaction ID - Shows transaction id of the current crosslink transaction. ■ MAC Address - Shows adjacent Node MAC addresses. ■ Link State - Shows AMF states of adjacent nodes on the link.
`Domain Nodes Tree`	Shows all the nodes in the domain: ■ Node - Name of the node in the domain. ■ Links on Node - Number of crosslinks on a vertex/node. ■ Link no - Shows adjacent Node names and Interface index. ■ Forwarding State - Shows state of AMF link Forwarding/Blocking.
`Crosslink Transaction Entries`	Shows all the transaction entries: ■ Node - Name of the AMF node. ■ Transaction ID - transaction id of the node. ■ Uplink Transaction ID - transaction id of the remote node.

Table 61-6: Parameter definitions from the show atmf links detail command output(cont.)

Parameter	Definition
`Uplink Information`	Show all uplink entries. ■ Waiting for Sync - Flag if uplinks are currently waiting for synchronization. ■ Transaction ID - Shows transaction id of the local node. ■ Number of Links - Number of up downlinks in the domain. ■ Number of Local Uplinks - Number of uplinks on this node to the parent domain. ■ Originating Node - Node originating the uplink information. ■ Domain - Name of the parent uplink domain. ■ Node - Name of the node in the parent domain, that is connected to the current domain. ■ Ifindex - Interface index of the parent node's link to the current domain. ■ VR ID - Virtual router id of the parent node's link to the current domain. ■ Transaction ID - Transaction identifier for the neighbor in crosslink. ■ Flags - Used in domain messages to exchange the state: ATMF_DOMAIN_FLAG_DOWN = 0 ATMF_DOMAIN_FLAG_UP = 1 ATMF_DOMAIN_FLAG_BLOCK = 2 ATMF_DOMAIN_FLAG_NOT_PRESENT = 4 ATMF_DOMAIN_FLAG_NO_NODE = 8 ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16 ATMF_DOMAIN_FLAG_NOT_LINKS = 32 ATMF_DOMAIN_FLAG_NO_CONFIG = 64 ■ Domain Controller - Domain Controller in the uplink domain ■ Domain Controller MAC - MAC address of Domain Controller in uplink domain
`Downlink Domain Information`	Shows all the downlink entries: ■ Domain - Name of the downlink domain. ■ Domain Controller - Controller of the downlink domain. ■ Domain Controller MAC - MAC address of the domain controller. ■ Number of Links - Total number of links to this domain from the Node. ■ Number of Links Up - Total number of links that are in UP state. ■ Number of Links on This Node - Number of links terminating on this node. ■ Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.
`Node Transaction List`	List of transactions from this downlink domain node. ■ Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain. ■ Transaction ID - Transaction id for this node. ■ Domain List: Shows list of nodes in the current domain and their links to the downlink domain.: ■ Domain - Domain name of the downlink node. ■ Node - Name of the node in the current domain. ■ Ifindex - Interface index for the link from the node to the downlink domain. ■ Transaction ID - Transaction id of the node in the current domain. ■ Flags - As mentioned above.

Table 61-6: Parameter definitions from the show atmf links detail command output(cont.)

Parameter	Definition
`Up/Downlink Ports Information`	Shows all the configured up and down link ports on this node: ■ Port - Name of the local port. ■ Ifindex - Interface index of the local port. ■ VR ID - Virtual router id for the local port. ■ Port Status - Shows status of the local port on the Node as UP/DOWN. ■ Port State - AMF state of the local port. ■ Adjacent Node - nodename of the adjacent node. ■ Adjacent Internal ID - Unique node identifier of the remote node. ■ Adjacent Ifindex - Interface index for the port of adjacent AMF node. ■ Adjacent Board ID - Product identifier for the adjacent node. ■ Adjacent VR ID - Virtual router id for the port on adjacent AMF node. ■ Adjacent MAC - MAC address for the port on adjacent AMF node. ■ Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node. ■ Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node. ■ Port Forwarding State - Local port forwarding state Forwarding or Blocking. ■ Port BPDU Receive Count - count of AMF protocol PDU's received. ■ Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes. ■ Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived. ■ Port Last Message Response - response from the remote neighbor to our last hello packet.

Note

You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

Related Commands

no debug all
clear atmf links statistics
show atmf

show atmf links statistics

This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master nodes

Syntax `show atmf links statistics [interface [<port_number>]]`

Parameter	Description
`interface`	Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports will be displayed.
<port_number>	Enter the port number for which statistics are required. A port range or a static channel can also be specified. Where no port number is specified, statistics will be displayed for all ports on the switch.

Mode User Exec

Example 1 To display AMF link statistics for the whole switch, use the command:

```
switch1# show atmf links statistics
```

Figure 61-14: Sample output from the show atmf links statistics command

```
switch1# show atmf links statistics

ATMF Statistics:

                                    Receive           Transmit
-------------------------------------------------------------------
Crosslink Hello                      7                 14
Crosslink Hello Domain               18                38
Crosslink Hello Uplink               3                 12
Hello Link                           32                31
Hello Neighbor                       55                57
Hello Stack                          0                 0
Database Description                 12                112
Database Request                     5                 4
Database Reply                       0                 5
Database Update                      35                9
Database Update Bitmap               0                 10
Database Acknowlegde                 112               74
Transmit Fails                       0                 0
Discards                             0                 0
Total AMF Packets                    300               366

ATMF Database Statistics:

Database Entries                     18
Database Full Ages                   0

ATMF Packet Discards:

Type0      0              Type1      0              Type2      0
Type3      0              Type4      0              Type5      0
Type6      0              Type7      0              Type8      0
Type9      0              Type10     0              Type11     0
Type12     0              Type13     0              Type14     0
Type15     0              Type16     0              Type17     0
Type18     0              Type19     0              Type20     0
Type21     0              Type22     0
```

Table 61-7: Parameter definitions from the show atmf links statistics command output

Parameter	Definition
`Receive`	Shows a count of AMF protocol packets received per message type.
`Transmit`	Shows the number of AMF protocol packets transmitted per message type.
`Database Entries`	Shows the number of AMF elements existing in the distributed database.
`Database Full Ages`	Shows the number of times the entries aged in the database.
`ATMF Packet Discards`	Shows the number of discarded packets of each type: ■ Type0: The number of discarded crosslink hello msgs received on a non crosslink port. ■ Type1: The number of discarded tx update packets - bad checksum. ■ Type2: The number of discarded tx update bitmap packets - bad checksum. ■ Type3: The number of discarded tx update packets - neighbor not in the correct state. ■ Type4: The number of discarded update packets - bad checksum. ■ Type5: The number of discarded update packets - neighbor not in the correct state. ■ Type6: The number of discarded update bitmap packets - bad checksum. ■ Type7: The number of discarded crosslink hello msgs received on a non crosslink port. ■ Type8: The number of discarded crosslink hello msg received on a port that is not in the correct state. ■ Type9: The number of discarded crosslink domain hello msgs received on a non crosslink port. ■ Type10: The number of discarded crosslink domain hello msgs received on a port that is not in the correct state. ■ Type11: The number of crosslink uplink hello msgs received on a non crosslink port. ■ Type12: The number of discarded crosslink uplink hello msgs ignored on a port that is not in the correct state. ■ Type13: The number of messages with an incorrect name for this AMF network. ■ Type14: The number of over-long packets received on a port. ■ Type15: The number of messages with a bad protocol version received on a port. ■ Type16: The number of messages with a bad packet checksum calculation received on a port. ■ Type17: The number of messages with a bad authentication type received on a port. ■ Type18: The number of messages with a bad simple password received on a port. ■ Type19: The number of discarded packets with an unsupported authentication type received on a port. ■ Type20: The number of discarded packets with an unknown neighbor received on a port.

Note

You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

Related Commands

no debug all
clear atmf links statistics
show atmf

show atmf memory

This command displays a summary of the AMF memory usage. It can only be run on AMF master nodes.

Syntax `show atmf memory`

Mode User Exec

Example To display AMF memory allocations on Node_1, use the command:

```
node_1# show atmf memory
```

Figure 61-15: Sample output from the show atmf memory command

```
node_1#show atmf memory

ATMF Memory Allocation:

Total memory allocated   : 30020 (bytes)
Total memory allocations : 77
 Line   1238  number      1  memory         28 (bytes)
 Line    244  number      2  memory         88 (bytes)
 Line   3753  number      2  memory       1872 (bytes)
 Line   1616  number      8  memory        320 (bytes)
 Line   1391  number      1  memory         60 (bytes)
 Line   1837  number     15  memory        600 (bytes)
 Line    288  number      1  memory      17716 (bytes)
 Line   3916  number      1  memory       1520 (bytes)
 ...
 Line   4205  number      1  memory       1520 (bytes)
 Line    206  number      4  memory       1524 (bytes)
 Line    549  number      1  memory        232 (bytes)
 Line   3495  number      1  memory         56 (bytes)
 Line   2628  number      2  memory         72 (bytes)
 Line    678  number      1  memory         32 (bytes)
 Line   1423  number      1  memory         48 (bytes)
 Line   1733  number      3  memory        492 (bytes)
 Line   1611  number      8  memory        256 (bytes)

ATMF Memory Deallocation:

Total memory deallocated   : 4958 (bytes)
Total memory deallocations : 45
 Line   1395  number      4  memory        400 (bytes)
 Line   1956  number      1  memory        164 (bytes)
 Line   1247  number      1  memory         52 (bytes)
 Line    876  number      2  memory         80 (bytes)
 Line    166  number      1  memory        232 (bytes)
 Line    415  number      7  memory        587 (bytes)
 Line    418  number      3  memory        300 (bytes)
 Line    822  number      2  memory         80 (bytes)
 Line   2341  number      4  memory        160 (bytes)
 Line   3025  number      2  memory         88 (bytes)
 Line    144  number      3  memory       1596 (bytes)
 Line    146  number      6  memory        312 (bytes)
 Line   2349  number      4  memory        160 (bytes)
 Line   1111  number      1  memory         59 (bytes)
 Line   1393  number      4  memory        688 (bytes)


-----------------------------------------------------
Total memory in use        : 4958 (bytes)
Total memory items         : 45
```

show atmf nodes

This command displays all nodes currently configured within the AMF network. It displays a topographical representation of the network infrastructure.

Syntax `show atmf nodes`

Mode Privileged Exec

Example To display AMF information for all nodes in the AMF, use the command:

```
node_1# show atmf nodes
```

Figure 61-16: Sample output from the show atmf nodes command.

```
node1#show atmf nodes

Node Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone

  Node                Device             ATMF                              Node
  Name                Type               Master  SC  Parent                Depth
-------------------------------------------------------------------------------
  Building_1          AT-SBx8112           Y     C   -                      0
* Building_2          x900-12XT/S          Y     N   -                      0
  Bld1_Floor_1        SwitchBlade x908     N     S   Building_1             1
  Bld1_Floor_2        x600-24Ts/XP         N     N   Building_1             1
  Bld2_Floor_1        x610-24Ts-POE+       N     N   Building_1             1
  SW_Team1            x210-24GT            N     N   Bld1_Floor_2           2

Current ATMF node count 6
```

show atmf provision nodes

This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master nodes.

Syntax `show atmf provision nodes`

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. The command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

Example To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 61-17: Sample output from the show atmf provision nodes command

```
switch1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media ..............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                  : switch2
Date & Time                : 06-May-2014 & 23:25:44
Provision Path             : card:/atmf/provision_nodes

Boot configuration :
Current boot image         : x510-1766_atmf_backup.rel (file exists)
Backup  boot image         : x510-main-20140113-2.rel (file exists)
Default boot config        : flash:/default.cfg (file exists)
Current boot config        : flash:/abc.cfg (file exists)
Backup  boot config        : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file            : ./.configs/.sw_v2.lic
                           : ./.configs/.swfeature.lic
Certificate file           : card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands
atmf provision node create
atmf provision node clone
atmf provision node configure boot config
atmf provision node configure boot system
show atmf backup

show atmf tech

This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

Syntax `show atmf tech`

Mode Privileged Exec

Example To display output for all AMF commands, use the command:

```
NodeName# show atmf tech
```

Figure 61-18: Sample output from the show atmf tech command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : ATMF_NET
Node Name              : node1
Role                   : Master
Current ATMF Nodes     : 8

ATMF Technical information:

Network Name                          : ATMF_NET
Domain                                : node1's domain
Node Depth                            : 0
Domain Flags                          : 0
Authentication Type                   : 0
MAC Address                           : 0014.2299.137d
Board ID                              : 287
Domain State                          : DomainController
Domain Controller                     : node1
Backup Domain Controller              : node2
Domain controller MAC                 : 0014.2299.137d
Parent Domain                         : -
Parent Domain Controller              : -
Parent Domain Controller MAC          : 0000.0000.0000
Number of Domain Events               : 0
Crosslink Ports Blocking              : 0
Uplink Ports Waiting on Sync          : 0
Crosslink Sequence Number             : 7
Domains Sequence Number               : 28
Uplink Sequence Number                : 2
Number of Crosslink Ports             : 1
Number of Domain Nodes                : 2
Number of Neighbors                   : 5
Number of Non Broadcast Neighbors     : 3
Number of Link State Entries          : 1
Number of Up Uplinks                  : 0
Number of Up Uplinks on This Node     : 0
DBE Checksum                          : 84fc6
Number of DBE Entries                 : 0
Management Domain Ifindex             : 4391
Management Domain VLAN                : 4091
Management ifindex                    : 4392
Management VLAN                       : 4092
...
...
```

Table 61-8: Parameter definitions from the show atmf tech command

Parameter	Definition
ATMF Status	Shows status of AMF feature on the Node as Enabled/Disabled.
Network Name	The name of the AMF network to which this node belongs.
Node Name	The name assigned to the node within the AMF network.
Role	The role configured on the switch within the AMF - either master or member.
Current ATMF Nodes	A count of the AMF nodes in the AMF network.
Node Address	The identity of a node (in the format name.atmf) that enables its access it from a remote location.
Node ID	A unique identifier assigned to an AMF node.
Node Depth	The number of nodes in path from this node to the core domain.
Domain State	A node's state within an AMF Domain - either controller or backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between nodes of different domains (up/down links). VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. Management Subnet - the Network prefix for the subnet. Management IP Address - the IP address allocated for this traffic. Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. Domain Subnet - the Subnet address used for this traffic. Domain IP Address - the IP address allocated for this traffic. Domain Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)
Device Type	Shows the Product Series Name.
ATMF Master	Indicates the nodes membership of the core domain (membership is indicated by Y)
SC	Shows switch configuration: ■ C - Chassis (such as SBx8100 series) ■ S - Stackable (VCS) ■ N - Standalone
Parent	A node to which connects to the present node's uplink, i.e. one layer higher in the hierarchy.
Node Depth	Shows the number of nodes in path from the current node to the Core domain.

Note The **show atmf tech** command can produce very large output. For this reason only the most significant terms are defined in this table.

show atmf working-set

This command displays the nodes that form the current AMF working-set.

Syntax `show atmf working-set`

Mode Privileged Exec

Example To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

Figure 61-19: Sample output from the show atmf working-set command.

```
ATMF Working Set Nodes:
node1, node2, node3, node4, node5, node6
Working set contains 6 nodes
```

Related Commands **atmf working-set**
show atmf
show atmf group

show debugging atmf

This command shows the debugging modes status for AMF.

Syntax `show debugging atmf`

Mode User Exec and Global Configuration

Example To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Figure 61-20: Sample output from the show debugging atmf command.

```
node1# show debugging atmf
ATMF debugging status:
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

Related Commands **debug atmf packet**

show debugging atmf packet

This command shows details of AMF Packet debug command.

Syntax `show debugging atmf packet`

Mode User Exec and Global Configuration

Example To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Figure 61-21: Sample output from the show debugging atmf packet command.

```
ATMF packet debugging is on
=== ATMF Packet Debugging Parameters===
Node Name: x900
Port name: port1.0.1
Limit: 500 packets
Direction: TX
Info Level: Level 2
Packet Type Bitmap:
2. Crosslink Hello BPDU pkt with downlink domain info
3. Crosslink Hello BPDU pkt with uplink info
4. Down and up link Hello BPDU pkts
6. Stack hello unicast pkts
8. DBE request
9. DBE update
10. DBE bitmap update
```

Related Commands **debug atmf**
debug atmf packet

show running-config atmf

This command displays the running system information that is specific to AMF.

Syntax `show running-config atmf`

Mode User Exec and Global Configuration

Example To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

Note

You can manage your show output, or make it a more selective, by using a command modifier. For information on using show-command modifiers see **"Controlling "show" Command Output" on page 1.35**.

Related Commands **show running-config**
no debug all

switchport atmf-link

This command enables you to configure a port or aggregator to be an AMF uplink/downlink. Running this command will automatically place the port or aggregator into trunk mode.

Use the **no** variant of this command to remove any AMF-link that may exist for the selected port or aggregated link.

Syntax

```
switchport atmf-link
no switchport atmf-link
```

Mode Interface Configuration

Example To make a switchport 1.0.1 an AMF uplink, use the following commands

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```

type atmf node

This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax `type atmf node {join|leave}`

Parameter	Description
`join`	AMF node join event.
`leave`	AMF node leave event.

Mode Trigger Configuration

Caution **Only configure this trigger on one device because it is a network wide event.**

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
========

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------


==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!


============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related Commands **show trigger**

undebug atmf

This command is an alias for the **no variant of the debug atmf** command on page 61.50.

The IPv4 addresses shown may include those specified for documentation purposes in RFC 5737: 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24. These addresses should not be used for practical networks (other than for testing purposes), nor should they appear in any public network.

Chapter 62: NTP Introduction and Configuration

Introduction 62.2
Overview 62.2
NTP on the Switch 62.3
Troubleshooting 62.4
Configuration Example 62.5

Introduction

This chapter describes the Network Time Protocol (NTP) service provided by the switch, and how to configure and monitor NTP on the switch.

NTP is a protocol for synchronizing the time clocks on a collection of network devices using a distributed client/server mechanism. NTP uses UDP (User Datagram Protocol) as the transport mechanism. NTP evolved from the Time Protocol (RFC 868) and the ICMP Timestamp message (RFC 792).

NTP provides protocol mechanisms to specify the precision and estimated error of the local clock and the characteristics of the reference clock to which it may be synchronized.

For detailed information about the commands used to configure NTP, see **Chapter 63, NTP Commands**.

Overview

NTP uses a subnetwork with primary reference clocks, gateways, secondary reference clocks, and local hosts. These are organized into a hierarchy with the more accurate clocks near the top and less accurate ones near the bottom.

A number of primary reference clocks, synchronized to national standards, are connected to widely accessible resources (such as backbone gateways or switches) operating as primary time servers. The primary time servers use NTP between them to crosscheck clocks, to mitigate errors due to equipment or propagation failures, and to distribute time information to local secondary time servers. The secondary time servers redistribute the time information to the remaining local hosts.

The hierarchical organization and distribution of time information reduces the protocol overhead, and allows selected hosts to be equipped with cheaper but less accurate clocks. NTP provides information which organizes this hierarchy on the basis of precision or estimated error.

- An NTP entity may be in one of the following operating modes; however, the switch's implementation of NTP supports two modes: client and server.
- An NTP entity operating in a client mode sends periodic messages to its peers, requesting synchronization by its peers.
- An NTP entity enters the server mode temporarily when it receives a client request message from one of its peers, and remains in server mode until the reply to the request has been transmitted.
- An NTP entity operating in symmetric active mode sends messages announcing its willingness to synchronize and be synchronized by its peers.
- An NTP entity enters symmetric passive mode in response to a message from a peer operating in Symmetric Active mode. An NTP entity operating in this mode announces its willingness to synchronize and be synchronized by its peers.
- An NTP entity operating in broadcast mode periodically sends messages announcing its willingness to synchronize all of its peers but not to be synchronized by any of them.

The same message format is used for both requests and replies. When a request is received, the server interchanges addresses and ports, fills in or overwrites certain fields in the message, recalculates the checksum, and returns it immediately. The information included in the NTP message allows each client/ server peer to determine the timekeeping characteristics of its peers, including the expected accuracies of their clocks. Each peer uses this information and selects the best time from possibly several other clocks, updates the local clock, and estimates its accuracy.

There is no provision in NTP for peer discovery, acquisition, or authentication. Data integrity is provided by the IP and UDP checksums. No reachability, circuit-management, duplicate-detection, or retransmission facilities are provided or necessary.

By its very nature clock synchronization requires long periods of time (hours or days) and multiple comparisons in order to maintain accurate timekeeping. The more comparisons performed, the greater the accuracy of the timekeeping.

NTP on the Switch

The implementation of NTP on the switch is based on the following RFCs:

- RFC 958, Network Time Protocol (NTP)
- RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1510, The Kerberos Network Authentication Service (V5)

Two modes of operation are supported: client and server. The switch is in client mode most of the time where it polls the configured peer at least once every preconfigured minimum time period.

The peer that the switch refers to must be a more accurate clock source than the switch itself or another switch directly connected to a more accurate clock source. The switch operates as a secondary time server. It cannot operate as a primary time server unless the primary clock source is operating in server mode. A primary clock source usually operates in broadcast mode, which is not supported by the switch's implementation of NTP. When the switch receives a valid reply from the peer, it synchronizes its own internal clock according to the information from the reply.

If the switch receives a synchronization request from an NTP client, it temporarily changes to server mode. It replies to the request with the current time from the switch's internal clock along with other information useful for synchronization. The switch's internal clock is accurate to 0.005 seconds.

Troubleshooting

Problem The switch is not assigning the time to devices on the LAN.

Solutions

- Check that the NTP peer's IP address is entered correctly.
- Check that the NTP peer can reach the switch, by pinging the switch from the NTP peer.

Problem The switch's clock does not synchronize with the NTP peer.

Solution

- The switch's clock can synchronize with the NTP peer only when its initial time is similar to the NTP peer's time (after setting the UTC offset). Manually set the switch's time so that it is approximately correct, and enable NTP again.
- Check that the UTC offset is correct.

Problem The switch's time is incorrect, even though it assigns the correct time to devices on the LAN.

Solution The UTC offset is probably incorrect, or needs to be adjusted for the beginning or end of summer time.

Configuration Example

NTP requires the IP module to be enabled and configured correctly.

The switch's implementation of NTP supports two modes: client and server mode. When a synchronization request is received from a client (e.g. a PC on a LAN), the switch enters server mode and responds with time information derived from the switch's own internal clock. Periodically the switch enters client mode, sending synchronization requests to a predefined peer to synchronize its own internal clock. The peer is assumed to be a primary clock source or another switch connected directly to a primary clock source.

This example illustrates how to configure two switches, one at a Head Office and one at a Regional Office, to provide a network time service. The Head Office switch is connected to a primary time server and provides the most accurate time information. The switch at the Regional Office uses the Head Office switch as its peer to avoid the cost of an additional WAN connection but provides slightly less accurate time information.

To configure NTP on the switch, the NTP module must be enabled and an NTP peer must be defined. NTP transfers time information in UTC format.

To set the switch to automatically change the time when summer time starts and ends, enable a summer time offset setting.

Example configuration parameters for a network time service:

Site	Regional Office	Head Office
Switch name	RG1	HO1
IP Address of Switch	10.5.35.114	10.12.25.4
IP Address of Peer	10.5.35.113	172.16.7.3

Step 1: Enable NTP and define the NTP peer.

The NTP feature must be enabled on all switches that are to provide a network time service. Each switch must have a peer defined where the switch synchronizes its own internal clock. Enable NTP on the Head Office switch and specify a primary time server as the peer by using the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 172.16.7.3
```

Note that you can also specify an IPv6 address for an NTP peer:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
```

Step 2: Configure the NTP parameters.

On each switch, the offset of local time from UTC time must be specified. In this example, both switches are in the same time zone, which is 12 hours ahead of UTC time. Use the following commands on both switches:

```
awplus(config)# clock timezone utc plus 12
```

Note that the range of offset is `<0-12>`.

Step 3: Check the NTP configuration.

Check the NTP configuration on each switch by using the command:

```
awplus# show ntp status
```

This command displays the following information on the Head Office switch.

```
Clock is synchronized, stratum 0, actual frequency is 0.0000
Hz, precision is 20 reference time is 00000000.00000000
(6:28:16.000 UTC Fri Feb  7 2036)clock offset is 0.000 msec,
root delay is 0.000 msec root dispersion is 0.000 msec,
```

Chapter 63: NTP Commands

Command List 63.2
ntp access-group 63.2
ntp authenticate 63.3
ntp authentication-key 63.4
ntp broadcastdelay 63.5
devicentp master 63.6
ntp peer 63.7
ntp server 63.9
ntp source 63.11
ntp trusted-key 63.13
show counter ntp 63.14
show ntp associations 63.15
show ntp status 63.16

Command List

This chapter provides an alphabetical reference for commands used to configure the Network Time Protocol (NTP). For more information, see **Chapter 62, NTP Introduction and Configuration**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

ntp access-group

This command creates an NTP access group, and applies a basic IP access list to it. This allows you to control access to NTP services.

The **no** variant of this command removes the configured NTP access group.

Syntax

```
ntp access-group [peer|query-only|serve|serve-only] [<1-99>|
    <1300-1999>]

no ntp access-group [peer|query-only|serve|serve-only]
```

Parameter	Description
`peer`	Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
`query-only`	Allows only NTP control queries from a system whose address passes the access list criteria.
`serve`	Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
`serve-only`	Allows only time requests from a system whose address passes the access list criteria.
<1-99>	Standard IP access list.
<1300-1999>	Expanded IP access list.

Mode Global Configuration

Examples To create an NTP peer access group for an extended IP access list, use the commands:

```
awplus# configure terminal
awplus(config)# ntp access-group peer 1998
```

To disable the NTP peer access group created above, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp access-group peer
```

ntp authenticate

This command enables NTP authentication. This allows NTP to authenticate the associations with other systems for security purposes.

The **no** variant of this command disables NTP authentication.

Syntax

```
ntp authenticate
no ntp authenticate
```

Mode Global Configuration

Examples To enable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# ntp authenticate
```

To disable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authenticate
```

ntp authentication-key

This command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently, the only key type supported is MD5.

The **no** variant of this disables the authentication key assigned previously using **ntp authentication-key**.

Syntax

```
ntp authentication-key <keynumber> md5 <key>
no ntp authentication-key <keynumber> md5 <key>
```

Parameter	Description
<keynumber>	*<1-4294967295>* The key number.
<key>	The authentication key.

Mode Global Configuration

Examples To define an authentication key number `134343` and a key value `mystring`, use the commands:

```
awplus# configure terminal
awplus(config)# ntp authentication-key 134343 md5 mystring
```

To disable the authentication key number `134343` with the key value `mystring`, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authentication-key 134343 md5 mystring
```

ntp broadcastdelay

Use this command to set the estimated round-trip delay for broadcast packets.

Use the **no** variant of this command to reset the round-trip delay for broadcast packets to the default offset of 0 microseconds.

Syntax

```
ntp broadcastdelay <delay>
no ntp broadcastdelay
```

Parameter	Description
<delay>	*<1-999999>* The broadcast delay in microseconds.

Default 0 microsecond offset, which can only be applied with the **no** variant of this command.

Mode Global Configuration

Examples To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:

```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```

To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:

```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```

devicentp master

Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source. Note that no stratum number is set by default.

Use the **no** variant of this command to stop the device being the designated NTP server.

Syntax

```
ntp master [<stratum>]
no ntp master
```

Parameter	Description
<stratum>	*<1-15>* The stratum number defines the configured level that is set for this master within the NTP hierarchy.

Mode Global Configuration

Usage The stratum number is null by default and must be set using this command. The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: **www.ntp.org//**

Examples To stop the device from being the designated NTP server use the commands:

```
awplus# configure terminal
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2 use the commands:

```
awplus# configure terminal
awplus(config)# ntp master 2
```

ntp peer

Use this command to configure an NTP peer association. An NTP association is a peer association if this system is willing to either synchronize to the other system, or allow the other system to synchronize to it.

Use the **no** variant of this command to remove the configured NTP peer association.

Syntax

```
ntp peer {<peeraddress>|<peername>}
ntp peer {<peeraddress>|<peername>} [prefer] [key <key>]
[version <version>]
no ntp peer {<peeraddress>|<peername>}
```

Parameter	Description
<peeraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X:X` for an IPv6 address.
<peername>	Specify the peer hostname. The peer hostname can resolve to an IPv4 and an IPv6 address.
`prefer`	Prefer this peer when possible.
`key` *<key>*	*<1-4294967295>* Configure the peer authentication key.
`version` *<version>*	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of `192.0.2.23`:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of `192.0.2.23`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of `2001:0db8:010d::1`:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key
                1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of `2001:0db8:010d::1`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

Related Commands **ntp server**
ntp source

ntp server

Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa.

Use the **no** variant of this command to remove the configured NTP server.

Syntax

```
ntp server {<serveraddress>|<servername>}
ntp server {<serveraddress>|<servername>} [prefer] [key <key>]
   [version <version>]
no ntp server {<serveraddress>|<servername>}
```

Parameter	Description
<serveraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.
<servername>	Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.
`prefer`	Prefer this server when possible.
`key` *<key>*	*<1-4294967295>* Configure the server authentication key.
`version` *<version>*	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of `192.0.1.23`:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of `192.0.1.23`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```

See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of `2001:0db8:010e::2`:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 22001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of `2001:0db8:010e::2`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

Related Commands **ntp peer**
ntp source

ntp source

Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Use the **no** variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

Syntax

```
ntp source <source-address>
no ntp source
```

Parameter	Description
<source-address>	Specify the IP address of the NTP source interface, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.

Default An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or is an invalid IP address.

Mode Global Configuration

Usage Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server determined by the **ntp peer** and **ntp server** commands.

Examples To configure the NTP source interface with the IPv4 address `192.0.1.23`, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.1.23
```

To configure the NTP source interface with the IPv6 address `2001:0db8:010e::2`, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 2001:0db8:010e::2
```

To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp source
```

Related Commands **ntp peer**
ntp server

ntp trusted-key

This command defines a list of trusted authentication keys. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

Use the **no** variant of this command to remove a configured trusted authentication key.

Syntax

```
ntp trusted-key <1-4294967295>
no ntp trusted-key <1-4294967295>
```

Parameter	Description
<*1-4294967295*>	The specific key number.

Mode Global Configuration

Examples To define a trusted authentication key numbered `234675`, use the following commands:

```
awplus# configure terminal
awplus(config)# ntp trusted-key 234676
```

To remove the trusted authentication key numbered `234675`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp trusted-key 234676
```

show counter ntp

This command displays packet counters for NTP.

Syntax `show counter ntp`

Mode User Exec and Privileged Exec

Output **Figure 63-1: Example output from the show counter ntp command**

```
NTP counters
Pkts Sent               ......... 0
Pkts Received           ......... 70958
Pkts Processed          ......... 0
Pkts current version    ......... 0
Pkts old version        ......... 0
Pkts unknown version    ......... 0
Pkts access denied      ......... 70958
Pkts bad length         ......... 0
Pkts bad auth           ......... 0
Pkts rate exceed        ......... 0
```

Table 63-1: Parameters in the output from the show counter ntp command

Parameter	Description
`Pkts Sent`	Total number of NTP client and server packets sent by your device.
`Pkts Received`	Total number of NTP client and server packets received by your device.
`Pkts Processed`	The number of packets processed by NTP. NTP processes a packet once it has determined that the packet is valid by checking factors such as the packet's authentication, format, access rights and version.
`Pkts current version`	The number of version 4 NTP packets received.
`Pkts old version`	The number of NTP packets received that are from an older version, down to version 1, of NTP. NTP is compatible with these versions and processes these packets.
`Pkts unknown version`	The number of NTP packets received that are an earlier version than version 1, or a higher version than version 4. NTP cannot process these packets.
`Pkts access denied`	The number of NTP packets received that do not match any access list statements in the NTP access-groups. NTP drops these packets.
`Pkts bad length`	The number of NTP packets received that do not conform to the standard packet length. NTP drops these packets.
`Pkts bad auth`	The number of NTP packets received that failed authentication. NTP drops these packets. Packets can only fail authentication if NTP authentication is enabled with the **ntp authenticate** command.
`Pkts rate exceed`	The number of packets dropped because the packet rate exceeded its limits.

Example To display counters for NTP, use the command:

```
awplus# show counter ntp
```

show ntp associations

Use this command to display the status of NTP associations. Use the detail option for displaying detailed information about the associations.

Syntax `show ntp associations [detail]`

Mode User Exec and Privileged Exec

Example See the sample output of the **show ntp associations** and **show ntp associations detail** commands displaying the status of NTP associations.

Figure 63-2: Example output from the show ntp associations command

```
awplus#show ntp associations
  address          ref clock       st  when  poll reach   delay  offset    disp
 ~192.0.2.23       INIT            16     -   512   000     0.0     0.0     0.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
awplus#
```

Figure 63-3: Example output from the show ntp associations detail command

```
awplus#show ntp associations detail
192.0.2.23 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
our mode client, peer mode unspec, our poll intvl 512, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-19,
org time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
rcv time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
xmt time cf11f2a4.cedde5e4 (00:39:00.808 UTC Tue Feb  2 2010)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filtoffset =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filterror =  16000.00  16000.00  16000.00  16000.00  16000.00  16000.00  16000.0
0  16000.00
```

Table 63-2: Parameters in the output from the show ntp associations command

Parameter	Description
address	Peer IP address
ref clock	IP address for reference clock
st	Stratum. The number of hops between the server and the accurate time source.
poll	Time between NTP requests from the device to the server.
reach	Shows whether or not the NTP server responded to the last request.
delay	Round trip delay between the device and the server.
offset	Difference between the device clock and the server clock.
disp	Lowest measure of error associated with peer offset based on delay.

show ntp status

Use this command to display the status of the Network Time Protocol (NTP).

Syntax `show ntp status`

Mode User Exec and Privileged Exec

Example See the sample output of the **show ntp status** command displaying information about the Network Time Protocol.

Figure 63-4: Example output from the show ntp status command

```
awplus#sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.0
actual frequency is 0.0000 Hz, precision is 2**-19
reference time is cf11f3f2.c7c081a1 (00:44:34.780 UTC Tue Feb  2
2010)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 7947729.000 msec,
awplus#
```

Chapter 64: Dynamic Host Configuration Protocol (DHCP) Introduction

Introduction 64.2
DHCP 64.2
DHCP Relay Agents 64.2
Configuring the DHCP Client 64.3
DHCP Relay Agent Introduction 64.4
Configuring the DHCP Relay Agent 64.4
DHCP Relay Agent Information Option (Option 82) 64.5

Introduction

This chapter describes the Dynamic Host Configuration Protocol (DHCP) support provided by your device. This includes how to configure your device to:

- use the DHCP client to obtain IP addresses for its own interfaces
- act as a DHCP relay agent

DHCP

DHCP is widely used to dynamically assign host IP addresses from a centralized server that reduces the overhead of administrating IP addresses. DHCP helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts. DHCP centrally manages IP address assignment for a large number of subscribers.

DHCP is based on BOOTP, and is defined in RFC 2131. It extends the BOOTP mechanism by providing:

- a method for passing configuration information to hosts on a TCP/IP network
- automatic allocation of reusable network addresses
- other additional configuration options

DHCP is designed to interoperate with BOOTP clients and DHCP clients, without the BOOTP clients needing any change to their initialization software.

DHCP Relay Agents

DHCP relay agents pass BOOTP and DHCP messages between servers and clients. Networks where the DHCP or BOOTP server does not reside on the same IP subnet as its clients need the intermediate routers to act as relay agents. A maximum number of 400 DHCP relay agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP relay agents will not be successful.

Configuring the DHCP Client

You can configure an interface on your device with a static IP address, or with a dynamic IP address assigned using your device's DHCP client. When you use the DHCP client, it obtains the IP address for the interface, and other IP configuration parameters, from a DHCP server. To configure an interface and gain its IP configuration using the DHCP client, use the command:

```
awplus(config)# interface <ifname>
awplus(config-if)# ip address dhcp [client-id <interface>]
[hostname <hostname>]
```

The DHCP client supports the following IP configuration options:

- Option 1—the subnet mask for your device.
- Option 51—lease expiration time.

If an IP interface is configured to get its IP address and subnet mask from DHCP, the interface does not take part in IP routing until the IP address and subnet mask have been set by DHCP.

For information on configuring a static IP address on an interface, see the **ip address** command on page 25.11.

DHCP Relay Agent Introduction

DHCP relay agents pass BOOTP messages between servers and clients. Networks where the DHCP or BOOTP server does not reside on the same IP subnet as its clients need the routers attached to the subnet to act as DHCP relay agents.

Note that both BOOTP and DHCP use BOOTP messages, allowing DHCP relay agents to relay all their packets.

Your device's DHCP Relay Agent relays these message types:

- BOOTREQUEST messages originating from any of the device's interfaces to a user-defined destination
- BOOTREPLY messages addressed to BOOTP clients on networks directly connected to the device

The DHCP relay agent ignores BOOTREPLY messages addressed to clients on networks not directly connected to the device. The device treats these as ordinary IP packets for forwarding.

A BOOTREQUEST message is relayed via unicast.

The hops field in a BOOTP message records the number of DHCP relay agents the message has been through. If the value of the hops field exceeds a predefined threshold, the DHCP relay agent discards the message.

Configuring the DHCP Relay Agent

To enable the DHCP relay agent on your device, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

Note DHCP relay agent is enabled by default on your switch. You only need to enter a `service dhcp-relay` command if DHCP relay agent is disabled on your switch.

You must define a relay destination on one of the device's interfaces before the relay agent can relay packets. This is the path to the DHCP server. To define a relay destination on the currently specified interface, on which there are DHCP clients, use the commands:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay server-address <ip-address>
```

You can define more than one relay destination on your device. The following table describes how the DHCP relay agent forwards the packets.

If an interface has...	Then the relay agent relays BOOTP packets it receives on that interface to...
one relay destination defined	the relay destination.
multiple relay destinations defined	each defined relay destination.

To delete a DHCP relay destination, use the command:

```
awplus(config-if)# no ip dhcp-relay server-address <ip-address>
```

See the **ip dhcp-relay server-address** command on page 65.13 and the **service dhcp-relay** command on page 65.15 for command description and command examples..

When the 'hops' field in a BOOTP message exceeds a predefined threshold the BOOTP message is discarded. The default of the threshold is 10. To set the threshold, use the command:

```
awplus(config-if)# ip dhcp-relay maxhops <1-255>
```

To display the current configuration of the DHCP relay agent, use the command:

```
awplus# show ip dhcp-relay [interface <interface-name>]
```

DHCP Relay Agent Information Option (Option 82)

You can use DHCP Relay Agent Information Option (Option 82) to protect your switch from spoofing attacks, where untrusted hosts can send requests for IP addresses to access the network. The switch relays these requests to DHCP servers and the servers send IP address leases in response. Untrusted hosts could then use these IP addresses for spoofing attacks. Option 82 contains information about the location of a DHCP client for the DHCP server.

Enabling the DCHP Relay Agent Information Option feature on the switch allows the switch to insert extra information into the DHCP packets that it is relaying. This information enables accurate identification of a subscriber, as it states which interface on which relay switch the subscriber is connected to. The information is stored in an optional field in the DHCP packet header, the relay agent-information option field, with the option ID 82.

The DHCP relay agent inserts the Option 82 information into the DHCP packets that it is relaying to a DHCP server. DHCP servers that are configured to recognize Option 82 may use the information to implement IP addresses, or other parameter assignment policies, based on the network location of the client device. Alternatively, the server can simply log this information to create a detailed audit trail of the locations of the clients to which given addresses were allocated at given times.

If Option 82 insertion is enabled, then the DHCP packet flow is as follows:

- The DHCP client generates a DHCP request and broadcasts it on the network.
- The DHCP relay agent intercepts the broadcast DHCP request packet and inserts the Option 82 field in the packet.
- The DHCP relay agent unicasts the DHCP request that includes the Option 82 field to the DHCP server.
- The DHCP server receives the packet.
- If the DHCP server supports Option 82, then it echoes the Option 82 field in the DHCP reply. If the server does not support Option 82, it ignores the option and does not echo it in the reply.
- The DHCP server unicasts the reply to the relay agent.
- The relay agent removes the Option 82 field and forwards the packet to the switch port connected to the DHCP client that sent the DHCP request.

For information about DHCP Relay Agent Information Option (Option 82), see RFC 3046.

To enable the relay agent to insert its details into the Option 82 field in requests received from clients on a particular interface, use the command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option
```

The Option 82 field contains sub-options. You can specify a value for the Remote ID sub-option, which contains information that identifies the host. To specify a value for the Remote ID, use the command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option remote-id
<remote-id>
```

If a Remote ID value is not specified, the Remote ID sub-option is set to the switch's MAC address. You can also configure the Remote ID value as an alphanumeric string.

Note that the Option 82 agent information added by DHCP Relay differs from the information inserted by DHCP snooping (see **"DHCP Relay Agent Option 82" on page 55.4**).

Dealing with client-originated packets that already contain Option 82 information

It is possible for the requests arriving from the clients to the relay agent to already contain Option 82 data. There are two main circumstances in which this can occur:

1. A client is maliciously inserting bogus information into the packet in an attempt to subvert the process of identifying the client's location. In this case, you would want to drop the packets that contain the bogus information (or remove bogus information).

2. A Layer 2 DHCP snooping switch, that sits between the clients and the DCHP relay, is validly inserting the Option 82 information into the packets. The DHCP snooping switch is not acting as a relay agent, but is inserting the Option 82 information. In this case, you would want to forward the valid information to the DHCP server.

The action taken on packets with an Option 82 field is configurable. The command to configure this action is shown below:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay information policy
{append|drop|keep|replace}
```

This command sets the action that the DHCP relay takes when a received DHCP client request contains Option 82 information. Required parameters configure the switch to:

- Leave the existing Option 82 field untouched (`keep` parameter)
- Append its own Option 82 field after the existing field (`append` parameter - use this when there is a trusted DHCP Snooping switch or another relay device between the clients and the DHCP Relay)
- Drop the packet (`drop` parameter)
- Replace the existing Option 82 information with its own (the default - `replace` parameter).

See the **ip dhcp-relay information policy** command on page 65.8 for a command description and command examples.

Checking Option 82 information in DHCP server responses

To configure the switch to check for the presence of Option 82 information in response packets returned from DHCP servers, configure DHCP-relay agent-option checking with the Interface Configuration command:

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay agent-option checking
```

This command enables the DHCP Relay Agent to check Option 82 information in response packets returned from DHCP servers. If the information does not match the information it has configured for its own client (downstream) interface then the DHCP relay agent drops the packet.

See the **ip dhcp-relay agent-option checking** command on page 65.6 for a command description and command examples.

Option 82 maximum message length

When 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, of the **ip dhcp-relay max-message-length** command then the DHCP relay will drop the packet.

```
awplus(config)# interface <interface-name>
awplus(config-if)# ip dhcp-relay max-message-length <548-1472>
```

Chapter 65: Dynamic Host Configuration Protocol (DHCP) Commands

Command List 65.2
ip address dhcp 65.3
ip dhcp-relay agent-option 65.4
ip dhcp-relay agent-option checking 65.6
ip dhcp-relay agent-option remote-id 65.7
ip dhcp-relay information policy 65.8
ip dhcp-relay maxhops 65.10
ip dhcp-relay max-message-length 65.11
ip dhcp-relay server-address 65.13
service dhcp-relay 65.15
show counter dhcp-client 65.16
show counter dhcp-relay 65.17
show dhcp lease 65.19
show ip dhcp-relay 65.20

Command List

This chapter provides an alphabetical reference for commands used to configure DHCP. For more information, see **Chapter 64, Dynamic Host Configuration Protocol (DHCP) Introduction**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

ip address dhcp

This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The **client-id** and **hostname** parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 51 - lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

Syntax

```
ip address dhcp [client-id <interface>] [hostname <hostname>]
no ip address dhcp
```

Parameter	Description
<interface>	The name of the interface you are activating the DHCP client on. If you specify this, then the MAC address associated with the specified interface is sent to the DHCP server in the optional identifier field. Default: no default
<hostname>	The hostname for the DHCP client on this interface. Typically this name is provided by the ISP. Default: no default

Mode Interface Configuration for a VLAN interface.

Examples To set the interface `vlan10` to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address dhcp
```

To stop the interface `vlan10` from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip address dhcp
```

Related Commands **ip address**

Validation Commands **show running-config**
show ip interface

ip dhcp-relay agent-option

This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. and **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**

Note The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands **ip dhcp-relay agent-option** and **ip dhcp-relay information policy** have been configured.

Syntax

```
ip dhcp-relay agent-option
no ip dhcp-relay agent-option
```

Default DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage Use this command to alter the DHCP Relay Agent Option 82 setting when your switch is the first hop for the DHCP client. To limit the maximum length of the packet, use the **ip dhcp-relay max-message-length** command.

This command cannot be enabled if DHCP snooping is enabled on your switch (**service dhcp-snooping** command on page 56.24), and vice versa.

Examples To make the DHCP Relay Agent listening on `vlan15` append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip dhcp-relay agent-option
```

Related Commands

ip dhcp-relay agent-option remote-id
ip dhcp-relay information policy
ip dhcp-relay max-message-length
service dhcp-relay

ip dhcp-relay agent-option checking

This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that **ip dhcp-relay agent-option** must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (**ip dhcp-relay agent-option**), and
- DHCP Relay Agent is enabled on the switch (**service dhcp-relay**)

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. and **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**

Syntax

```
ip dhcp-relay agent-option checking
no ip dhcp-relay agent-option checking
```

Mode Interface Configuration for a VLAN interface.

Examples To make the DHCP Relay Agent listening on `vlan10` check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on `vlan10` from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related Commands

ip dhcp-relay agent-option
ip dhcp-relay agent-option remote-id
ip dhcp-relay information policy
service dhcp-relay

ip dhcp-relay agent-option remote-id

Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the switch's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. and **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**

Syntax

```
ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed.

Default The Remote ID is set to the switch's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (**ip dhcp-relay agent-option**), and
- DHCP Relay Agent is enabled on the switch (**service dhcp-relay**)

Examples To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

Related Commands
ip dhcp-relay agent-option
ip dhcp-relay agent-option checking
show ip dhcp-relay

ip dhcp-relay information policy

This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see **"DHCP Relay Agent Introduction" on page 64.4** and **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**

Note The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands **ip dhcp-relay agent-option** and **ip dhcp-relay information policy** have been configured.

Syntax

```
ip dhcp-relay information policy {append|drop|keep|replace}
no ip dhcp-relay information policy
```

Parameter	Description
`append`	The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.
`drop`	The DHCP Relay Agent discards the packet.
`keep`	The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.
`replace`	The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet.

Mode Interface Configuration for a VLAN interface.

Examples To make the DHCP Relay Agent listening on `vlan15` drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface `vlan15`, use

the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip dhcp-relay information policy
```

Related Commands **ip dhcp-relay agent-option**
ip dhcp-relay agent-option checking

ip dhcp-relay maxhops

This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. For Option 82 introductory information, see **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**.

Syntax

```
ip dhcp-relay maxhops <1-255>
no ip dhcp-relay maxhops
```

Parameter	Description
<1-255>	The maximum hop count value.

Default The default hop count threshold is 10 hops.

Mode Interface Configuration for a VLAN interface.

Example To set the maximum number of hops to 5 for packets received on interface `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay maxhops 5
```

Related Commands **service dhcp-relay**

ip dhcp-relay max-message-length

This command applies when the switch is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. For Option 82 introductory information, see **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**.

Syntax

```
ip dhcp-relay max-message-length <548-1472>
no ip dhcp-relay max-message-length
```

Parameter	Description
<548-1472>	The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes).

Default The default is 1400 bytes.

Mode Interface Configuration for a VLAN interface.

Usage When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a *request* packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

Note Before setting this command, you must first run the **ip dhcp-relay agent-option** command on page 65.4. This will allow the DHCP Relay Agent Option 82 fields to be appended.

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface `vlan7`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface `vlan7`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# no ip dhcp-relay max-message-length
```

Related Commands **service dhcp-relay**

ip dhcp-relay server-address

This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

For DHCP Relay Agent introductory information, see **"DHCP Relay Agent Introduction" on page 64.4**. For Option 82 introductory information, see **"DHCP Relay Agent Information Option (Option 82)" on page 64.5**.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

Syntax

```
ip dhcp-relay server-address <ip-address>
no ip dhcp-relay server-address <ip-address>
no ip dhcp-relay
```

Parameter	Description
<ip-address>	Specify the IPv4 address of the DHCP server for DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D.

Mode Interface Configuration for a VLAN interface.

Usage See also the **service dhcp-relay** command to enable the DHCP Relay Agent on your device. The **ip dhcp-relay server-address** command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

Examples To enable the DHCP Relay Agent to relay DHCP packets on interface `vlan2` to the DHCP server with the IPv4 address `192.0.2.200`, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address `192.0.2.200` from the list of servers available to the DHCP Relay Agent on interface `vlan2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To disable DHCP relay on `vlan10`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay
```

Related Commands **service dhcp-relay**

service dhcp-relay

This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

Syntax

```
service dhcp-relay
no service dhcp-relay
```

Mode Global Configuration

Usage A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

Default The DHCP-relay service is enabled by default.

Examples To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

Related Commands

ip dhcp-relay agent-option
ip dhcp-relay agent-option checking
ip dhcp-relay information policy
ip dhcp-relay maxhops
ip dhcp-relay server-address

show counter dhcp-client

This command shows counters for the DHCP client on your device.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show counter dhcp-client`

Mode User Exec and Privileged Exec

Example To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

Output **Figure 65-1: Example output from the show counter dhcp-client command**

```
show counter dhcp-client

DHCPDISCOVER out      ......... 10
DHCPREQUEST out       ......... 34
DHCPDECLINE out       ......... 4
DHCPRELEASE out       ......... 0
DHCPOFFER in          ......... 22
DHCPACK in            ......... 18
DHCPNAK in            ......... 0
```

Table 65-1: Parameters in the output of the show counter dhcp-client command

Parameter	Description
`DHCPDISCOVER out`	The number of DHCP Discover messages sent by the client.
`DHCPREQUEST out`	The number of DHCP Request messages sent by the client.
`DHCPDECLINE out`	The number of DHCP Decline messages sent by the client.
`DHCPRELEASE out`	The number of DHCP Release messages sent by the client.
`DHCPOFFER in`	The number of DHCP Offer messages received by the client.
`DHCPACK in`	The number of DHCP Acknowledgement messages received by the client.
`DHCPNAK in`	The number of DHCP Negative Acknowledgement messages received by the client.

Related Commands **ip address dhcp**

show counter dhcp-relay

This command shows counters for the DHCP Relay Agent on your device.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show counter dhcp-relay`

Mode User Exec and Privileged Exec

Examples To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

Output **Figure 65-2: Example output from the show counter dhcp-relay command**

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In               ......... 4
Replies In                ......... 4
Relayed To Server         ......... 4
Relayed To Client         ......... 4
Out To Server Failed      ......... 0
Out To Client Failed      ......... 0
Invalid hlen              ......... 0
Bogus giaddr              ......... 0
Corrupt Agent Option      ......... 0
Missing Agent Option      ......... 0
Bad Circuit ID            ......... 0
Missing Circuit ID        ......... 0
Bad Remote ID             ......... 0
Missing Remote ID         ......... 0
Option Insert Failed      ......... 0
```

Table 65-2: Parameters in the output of the show counter dhcp-relay command

Parameter	Description
`Requests In`	The number of DHCP Request messages received from clients.
`Replies In`	The number of DHCP Reply messages received from servers.
`Relayed To Server`	The number of DHCP Request messages relayed to servers.
`Relayed To Client`	The number of DHCP Reply messages relayed to clients.
`Out To Server Failed`	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
`Out To Client Failed`	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
`Invalid hlen`	The number of incoming messages dropped due to an invalid hlen field.
`Bogus giaddr`	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.

Table 65-2: Parameters in the output of the show counter dhcp-relay com-

Parameter	Description
`Corrupt Agent Option`	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command.
`Missing Agent Option`	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command.
`Bad Circuit ID`	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command
`Missing Circuit ID`	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command
`Bad Remote ID`	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command
`Missing Remote ID`	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the **ip dhcp-relay agent-option** command is configured for an interface. Messages generating the errors are only dropped if the **ip dhcp-relay agent-option checking** command is configured on the interface as well as the **ip dhcp-relay agent-option** command
`Option Insert Failed`	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: ■ the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the **ip dhcp-relay information policy** command. ■ there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.

show dhcp lease

This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show dhcp lease [<interface>]`

Parameter	Description
<interface>	Interface name to display DHCP lease details for.

Mode User Exec and Privileged Exec

Example To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for vlan1, use the command:

```
awplus# show dhcp lease vlan1
```

Output **Figure 65-3: Example output from the show dhcp lease command**

```
Interface vlan1
-----------------------------------------------------------------
IP Address:                   192.168.22.4
Expires:                      13 Mar 2007 20:10:19
Renew:                        13 Mar 2007 18:37:06
Rebind:                       13 Mar 2007 19:49:29
Server:
Options:
  subnet-mask                 255.255.255.0
  routers                     19.18.2.100,12.16.2.17
  dhcp-lease-time             3600
  dhcp-message-type           5
  domain-name-servers         192.168.100.50,19.88.200.33
  dhcp-server-identifier      192.168.22.1
  domain-name                 alliedtelesis.com

Interface vlan2
-----------------------------------------------------------------
IP Address:                   100.8.16.4
Expires:                      13 Mar 2007 20:15:39
Renew:                        13 Mar 2007 18:42:25
Rebind:                       13 Mar 2007 19:54:46
Server:
Options:
  subnet-mask                 255.255.0.0
  routers                     10.58.1.51
  dhcp-lease-time             1000
  dhcp-message-type           5
  dhcp-server-identifier      100.8.16.1
```

Related Commands **ip address dhcp**

show ip dhcp-relay

This command shows the configuration of the DHCP Relay Agent on each interface.

For information on output options, see **"Controlling "show" Command Output" on page 1.35**.

Syntax `show ip dhcp-relay [interface <interface-name>]`

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent's configuration on the interface `vlan100`, use the command:

```
awplus# show ip dhcp-relay interface vlan100
```

Output **Figure 65-4: Example output from the show ip dhcp-relay command**

```
DHCP Relay Service is enabled

vlan100 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers :   192.168.1.200
```

Related Commands
ip dhcp-relay agent-option
ip dhcp-relay agent-option checking
ip dhcp-relay information policy
ip dhcp-relay maxhops
ip dhcp-relay server-address

Chapter 66: SNMP Introduction

Introduction 66.2
Network Management Framework 66.2
Structure of Management Information 66.4
Names 66.5
Instances 66.6
Syntax 66.7
Access 66.7
Status 66.7
Description 66.7
The SNMP Protocol 66.8
SNMP Versions 66.8
SNMP Messages 66.9
Polling versus Event Notification 66.9
Message Format for SNMPv1 and SNMPv2c 66.10
SNMP Communities (Version v1 and v2c) 66.11
SNMPv3 Entities 66.11
SNMPv3 Message Protocol Format 66.12
SNMPv1 and SNMPv2c 66.13
SNMP MIB Views for SNMPv1 and SNMPv2c 66.13
SNMP Communities 66.13
Configuration Example (SNMPv1 and v2) 66.15
SNMPv3 ..... 66.18
SNMP MIB Views for SNMPv3 ..... 66.18
SNMP Groups 66.18
SNMP Users 66.18
Configuration Example (SNMPv3) 66.19
Using SNMP to Manage Files and Software 66.20
Copy a File to or from a TFTP Server 66.20
Upgrade Software and Configuration Files 66.22

Introduction

The Simple Network Management Protocol (SNMP) is the network management protocol of choice for the Internet and IP-based internetworks.

This chapter describes the main features of SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c) and Version 3 (SNMPv3). It also describes support for SNMP on the switch, and how to configure the switch's SNMP agent.

Unless a particular version of SNMP is named, "SNMP" in this chapter refers to versions SNMPv1, SNMPv2c and SNMPv3.

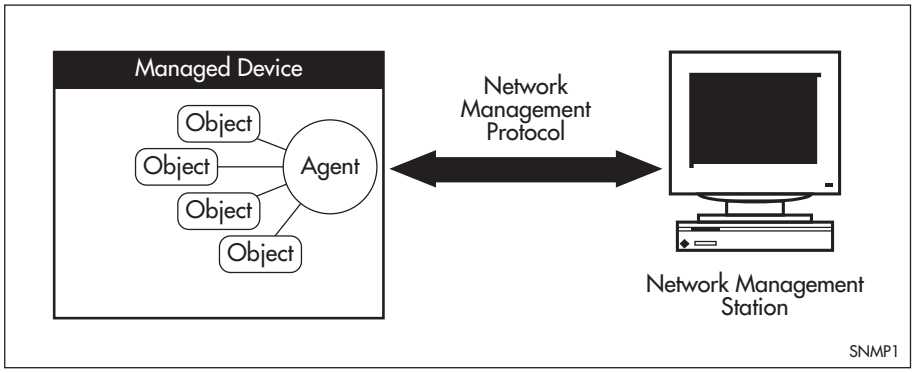
See also **Chapter 67, SNMP Commands** and **Chapter 68, SNMP MIBs**.

Network Management Framework

A network management system has the following components:

- One or more **managed devices**, each containing an agent that provides the management functions. A managed device may be any computing device with a network capability, for example, a host system, workstation, terminal server, printer, router, switch, bridge, hub or repeater.
- One or more **Network Management Stations (NMS)**. An NMS is a host system running a network management protocol and network management applications, enabling the user to manage the network.
- A **network management protocol** used by the NMS and agents to exchange information.

Figure 66-1: Components of a network management system



The Internet-standard Network Management Framework is the framework used for network management in the Internet. The framework was originally defined by the following documents:

- RFC 1155, *Structure and identification of management information for TCP/IP based internets* (referred to as the SMI), details the mechanisms used to describe and name the objects to be managed.
- RFC 1213, *Management Information Base for network management of TCP/ IP-based internets: MIB-II* (referred to as MIB-II), defines the core set of managed objects for the Internet suite of protocols. The set of managed objects can be extended by adding other MIBs specific to particular protocols, interfaces or network devices.
- RFC 1157, *A Simple Network Management Protocol (SNMP)*, is the protocol used for communication between management stations and managed devices.

Subsequent documents that have defined SNMPv2c are:

- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1903, *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1904, *Conformance Statements for Version 2 of the Simple Network Management Protocol*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1906, *Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*
- RFC 2580, *Conformance Statements for SMIv2*

Subsequent documents that have defined SNMPv3 are:

- RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*
- RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
- RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
- RFC 3413, *Simple Network Management Protocol (SNMP) Applications*
- RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
- RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
- RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

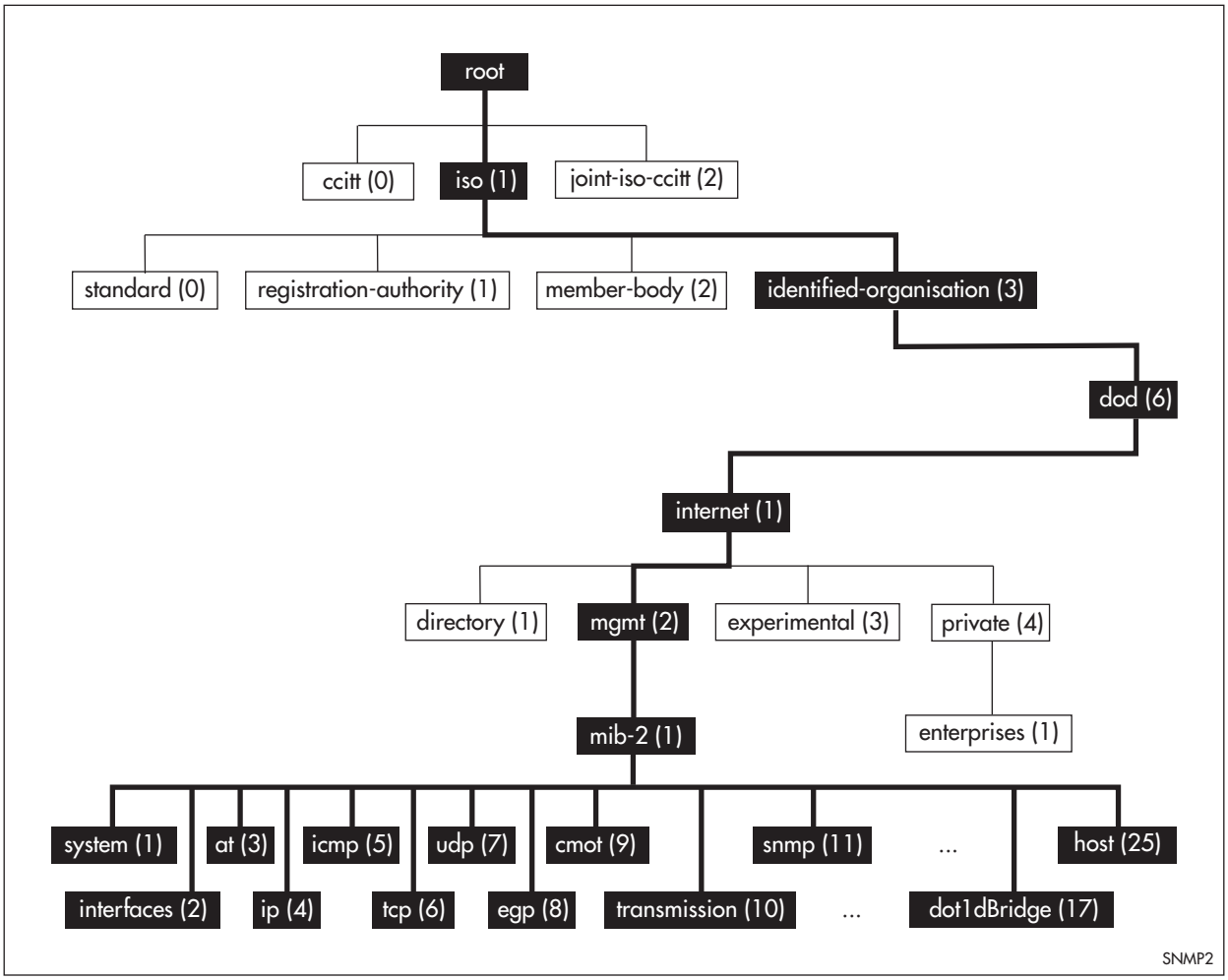
Structure of Management Information

The structure of management information (SMI) defines the schema for a collection of managed objects residing in a virtual store called the management information base (MIB). The information in a MIB includes administrative and operational configuration information, as well as counters of system events and activities.

The MIB is organized into a tree-like hierarchy in which nodes are each assigned an identifier consisting of a non-negative integer and an optional brief textual description.

Each managed object is represented by a leaf node and is defined by its name, syntax, access mode, status and description. It can also be specifically identified by its unique position within the tree. This position is expressed as a series of dot-delimited sub-identifiers that start at the root node and end in the sub-identifier at the particular object's leaf node. For example, in **Figure 66-2** the object named interfaces would be uniquely identified by the string of individual sub-identifiers, 1.3.6.1.2.1.2.

Figure 66-2: Top levels of the Internet-standard Management Information Base (MIB)



Objects defined in the Internet-standard MIB (MIB-II) reside in the mib(1) sub-tree.

Names

Names are used to identify managed objects, and are hierarchical in nature. An object identifier is a globally unique, authoritatively assigned sequence of non-negative integers which traverse the MIB tree from the root to the node containing the object.

Object identifiers may be represented in one of the following forms:

- Dotted notation lists the integer values found by traversing the tree from the root to the node in question, separated by dots. For example, the following identifies the MIB-II sub-tree:

  ```
  1.3.6.1.2.1
  ```

  The following identifies the sysDescr object in the system group of MIB-II:

  ```
  1.3.6.1.2.1.1.1
  ```

- Textual notation lists the textual descriptions found by traversing the tree from the root to the node in question, separated by spaces and enclosed in braces. The following example identifies the internet sub-tree:

  ```
  { iso org dod 1}
  ```

  The name may be abbreviated to a relative form. The following example identifies the first (directory) node of the internet sub-tree:

  ```
  { internet 1}
  ```

- Combined notation lists both the integer values and textual descriptions found by traversing the tree from the root to the node in question. The integer value is placed in parentheses after the textual description. The labels are separated by spaces and enclosed in braces. For example, the following identifies the first (directory) node in the internet sub-tree:

  ```
  {iso(1) org(3) dod(6) internet(1) 1}
  ```

  The name may be abbreviated to the following:

  ```
  directory(1)
  ```

Since there is no effective limit to the magnitude of non-negative integers, and no effective limit to the depth of the tree, the MIB provides an unlimited name space.

An object is also usually assigned an object descriptor. The object descriptor is a unique, mnemonic, printable string intended for humans to use when discussing the MIB.

Instances

Objects are just templates for data types. An actual value that can be manipulated by an NMS is an instance of an object. An instance is named by appending an instance identifier to the end of the object's object identifier. The instance identifier depends on the object's data type:

- If the object is not a column in a table, the instance identifier is 0 (zero). For example, the instance of the sysDescr object is:

  ```
  sysDescr.0
  or 1.3.6.1.2.1.1.1.0
  ```

- If the object is a column in a table, the method used to assign an instance identifier varies. Typically, the value of the index column or columns is used.

The object ifTable in MIB-II contains information about interfaces and is indexed by the interface number, ifIndex. The instance of the ifDescr object for the first interface is:

```
ifDescr.1
```

```
or 1.3.6.1.2.1.2.2.1.2.1
```

If the index column is an IP address, the entire IP address is used as the instance identifier. The object ipRouteTable in MIB-II contains information about IP routes and is indexed by the destination address, ipRouteDest. The instance of the ipRouteNextHop object for the route 131.203.9.0 is:

```
ipRouteNextHop.131.203.9.0
```

```
or 1.3.6.1.2.1.4.21.1.7.131.203.9.0
```

If the table has more than one index, the values of all the index columns are combined to form the instance identifier. The object tcpConnTable in MIB-II contains information about existing TCP connections and is indexed by the local IP address (tcpConnLocalAddress), the local port number (tcpConnLocalPort), the remote IP address (tcpConnRemAddress) and the remote port number (tcpConnRemPort) of the TCP connection. The instance of the tcpConnState object for the connection between 131.203.8.36,23 and 131.203.9.197,1066 is:

```
tcpConnState.131.203.8.36.23.131.203.9.197.1066
```

```
or 1.3.6.1.2.1.6.13.1.1.131.203.8.36.23.131.203.9.197.1066
```

Syntax

The syntax of an object describes the abstract data structure corresponding to that object type. For example, INTEGER or OCTET STRING.

Access

The access mode of an object describes the level of access for the object.

Access modes for MIB objects:

Access	Description
Read-only	The object's value can be read but not set.
Read-write	The object's value can be read and set.
Write-only	The object's value can be set but not read.
Not-accessible	The object's value cannot be read or set.

Status

The status of an object describes the implementation requirements for the object.

Status values for MIB objects:

Status	Description
Mandatory	Managed devices must implement the object.
Optional	Managed devices may implement the object.
Obsolete	Managed devices need no longer implement the object.
Deprecated	Managed devices should implement the object. However, the object may be deleted from the next version of the MIB. A new object with equal or superior functionality is defined.

Description

The definition of an object may include an optional textual description of the meaning and use of the object. This description is often essential for successful understanding of the object.

The SNMP Protocol

The SNMP protocol provides a mechanism for management entities, or stations, to extract information from the Management Information Base (MIB) of a managed device.

The normal method of accessing information in a MIB is to use a Network Management Station (NMS), typically a PC or workstation, to send commands to the managed device (in this case the switch) using the SNMP protocol.

SNMP can use a number of different protocols as its underlying transport mechanism, but the most common transport protocol, and the only one supported by the switch, is UDP. Therefore the IP module must be enabled and properly configured in order to use SNMP. SNMP trap messages are sent to UDP port 162; all other SNMP messages are sent to UDP port 161. The switch's SNMP agent accepts SNMP messages up to the maximum UDP length the switch can receive.

Other transport mappings have been defined (e.g. OSI [RFC 1418], AppleTalk [RFC 1419] and IPX [RFC 1420]), but the standard transport mapping for the Internet (and the one the switch uses) is UDP. The IP module must be enabled and configured correctly. See **Chapter 25, IP Addressing and Protocol Commands** for detailed descriptions of the commands required to enable and configure IP.

SNMP Versions

The switch supports SNMP version 1 (SNMPv1), SNMP version 2c (SNMPv2c) and SNMP Version 3 (SNMPv3). The three versions operate similarly.

SNMPv2c updated the original protocol, and offered the following main enhancements:

- a new format for trap messages.
- the get-bulk-request PDU allows for the retrieval of large amounts of data, including tables, with one message.
- more error codes mean that error responses to set messages have more detail than is possible with SNMPv1.
- three new exceptions to errors can be returned for get, get-next and get-bulk-request messages. These are: noSuchObject, noSuchInstance, and endOfMibView.

SNMPv3 provides significant enhancements to address the security weaknesses existing in the earlier versions. This is achieved by implementing two new major features:

- Authentication - by using password hashing and time stamping.
- Privacy - by using message encryption.

Support for multiple versions of SNMP is achieved by responding to each SNMP request with a response of the same version. For example, if an SNMPv1 request is sent to the switch, an SNMPv1 response is returned. If an SNMPv2c request is sent, an SNMPv2c response is returned. Therefore, authentication and encryption functions are not invoked when messages are detected as having either an SNMPv1 or SNMPv2c protocol format.

SNMP Messages

The SNMP protocol is termed simple because it has only six operations, or messages—get, get-next, get-response, set, and trap, and SNMPv2c also has the get-bulk-request message. The replies from the managed device are processed by the NMS and generally used to provide a graphical representation of the state of the network. The two major SNMP operations available to a management station for interacting with a client are the get and set operations. The SNMP set operator can lead to security breaches, since SNMP is not inherently very secure. When forced to operate in either SNMPv1 or v2 mode, when operating with older management stations for example, care must be taken in the choice and safe-guarding of community names, which are effectively passwords for SNMP.

Polling versus Event Notification

SNMP employs a polling paradigm. A Network Management Station (NMS) polls the managed device for information as and when it is required, by sending get-request, get-next-request, and/or get-bulk-request PDUs to the managed device. The managed device responds by returning the requested information in a get-response PDU. The NMS may manipulate objects in the managed device by sending a set-request PDU to the managed device.

The only time that a managed device initiates an exchange of information is in the special case of a trap PDU. A managed device may generate a limited set of traps to notify the NMS of critical events that may affect the ability of the NMS to communicate with the managed device or other managed devices on the network, and therefore to “manage” the network. Such events include the restarting or re-initialization of a device, a change in the status of a network link (up or down), or an authentication failure.

Message Format for SNMPv1 and SNMPv2c

Table 66-1: Fields in an SNMP message

Field	Function
Version	The version of the SNMP protocol. The value is version-1 (0) for the SNMP protocol as defined in RFC 1157, or version-2c (1) for the SNMP protocol as defined in RFC 1902.
Community	The name of an SNMP community, for authentication purposes
SNMP PDU	An SNMP Protocol Data Unit (PDU).

Table 66-2: SNMP PDUs

PDU	Function
get-request	Sent by an NMS to an agent, to retrieve the value of an object.
get-next-request	Sent by an NMS to an agent, to retrieve the value of the next object in the sub-tree. A sub-tree is traversed by issuing a get-request PDU followed by successive get-next-request PDUs.
get-bulk-request	Sent by an NMS to an agent to request a large amount of data with a single message. This is for SNMPv2c messages.
set-request	Sent by an NMS to an agent, to manipulate the value of an object. SNMP PDU Version Community
get-response	Sent by an agent to an NMS in response to a get-request, get-next-request, get-bulk-response, or set-request PDU.
trap	Sent by an agent to an NMS to notify the NMS of a extraordinary event.
report	Although not explicitly defined in the RFCs, reports are used for specific purposes such as EngineID discovery and time synchronization.

Table 66-3: Generic SNMP traps

Value	Meaning
coldStart	The agent is re-initializing itself. Objects may be altered.
warmStart	The agent is re-initializing itself. Objects are not altered.
linkDown	An interface has changed state from up to down.
linkUp	An interface has changed state from down to up.
authenticationFailure	An SNMP message has been received with an invalid community name.
egpNeighborLoss	An EGP peer has transitioned to down state.

SNMP Communities (Version v1 and v2c)

A community is a relationship between an NMS and an agent. The community name is used like a password for a trivial authentication scheme. Both SNMPv1 and SNMPv2c provide security based on the community name only. The concept of communities does not exist for SNMPv3, which instead provides for a far more secure communications method using entities, users, and groups.

Caution

We strongly recommend removing community membership from all SNMPv3 configured devices to prevent access to them via SNMPv1 and SNMv2c, which could bypass the additional SNMPv3 security features.

SNMPv3 Entities

Entities comprise one of the basic components of the SNMPv3 enhanced architecture. They define the functionality and internal structure of the SNMP managers and agents. An in-depth description of entities can be found in RFC 3411, on which the following text is based. SNMPv3 defines two entity types, a manager and an agent. Both entity types contain two basic components: an SNMP engine and a set of applications.

SNMP engine

The engine provides the basic services to support the agents component applications, in this respect it performs much of the functionality expected of the ISO Session and Presentation layers. These functions include message transmission and reception, authentication and encryption, and access control to its managed objects database (MIB). The SNMP engine comprises the following components:

- Dispatcher
- Message processing Subsystem
- Security Subsystem
- Access Control Subsystem

The only security subsystem presently supported is the user based security model (USM).

Each SNMP engine is identified by an snmpEngineID that must be unique within the management system. A one to one association exists between an engine and the entity that contains it.

Entity applications

The following applications are defined within the agent applications:

- Command Generator
- Notification Receiver
- Proxy Forwarder
- Command Responder
- Notification Originator
- Other

SNMPv3 Message Protocol Format

Table 66-4: SNMPv3 PDUs

Value	Meaning
msgVersion	Identifies the message format to be SNMPv3.
msgID	An identifier used between SNMP entities to coordinate message requests and responses. Note that a message response takes the msgID value of the initiating message.
msgMaxSize	Conveys the maximum message size (in octets) an integer between 484 and 2^{31}-1, supported by the sender of the message. Specified as msgFlags. A single octet whose last three bits indicate the operational mode for privacy, authentication, and report.
msgSecurityModel	An identifier used to indicate the security mode (i.e. SNMPv1, SNMPv2c or SNMPv3 to be used when processing the message. Note that although only the SNMPv3 identifier is accepted by the switch, these earlier version message formats are detected by the msgVersion field and processed appropriately.
msgAuthoritativeEngineID	The ID of the authoritative engine that relates to a particular message, i.e. the source engine ID for Traps, Responses and Reports, and the destination engine for Gets, GetNexts, Sets, and Informs.
msgAuthoritativeEngineBoots	A value that represents the number of times the authoritative engine has rebooted since its installation. Its value has the range 1 to 2^{31}-1.
msgAuthoritativeEngineTime	The number of seconds since the authoritative engine snmpEngineBoots counter was last incremented.
msgUserName	The name of the user (principal) on whose behalf the message is being exchanged.
msgAuthenticationParameters	If the message has been authenticated, this field contains a serialized OCTET STRING representing the first 12 octets of the HMAC-MD5-96 output done over the whole message.
msgPrivacyParameters	For encrypted data, this field contains the “salt” used to create the DES encryption Initialization Vector (IV).
ContextEngineID	Within a particular administrative domain, this field uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName
ContextName	A unique name given to a context within a particular SNMP entity.

SNMPv1 and SNMPv2c

Although software levels 2.6.3 and higher support the specific facilities of SNMP v1 and v2, their documentation is available to provide backward compatibility with older network management systems. The far superior security features offered by implementing SNMPv3 should be used wherever possible.

The switch's implementation of SNMPv1 is based on RFC 1157, *A Simple Network Management Protocol (SNMP)*, and RFC 1812, *Requirements for IP Version 4 Routers*.

When the SNMP agent is disabled, the agent does not respond to SNMP request messages. The agent is disabled by default. The current state and configuration of the SNMP agent can be displayed.

SNMP MIB Views for SNMPv1 and SNMPv2c

An SNMP MIB view is a arbitrary subset of objects in the MIB. Objects in the view may be from any part of the object name space, and not necessarily the same sub-tree. An SNMP community profile is the pairing of an SNMP access mode (read-only or read-write) with the access mode defined by the MIB for each object in the view. For each object in the view, the community profile defines the operations that can be performed on the object.

Pairing an SNMP community with an SNMP community profile determines the level of access that the agent affords to an NMS that is a member of the specified community. When an agent receives an SNMP message, it checks the community name encoded in the message. If the agent knows the community name, the message is deemed to be authentic and the sending SNMP entity is accepted as a member of the community. The community profile associated with the community name then determines the sender's view of the MIB and the operations that can be performed on objects in the view.

SNMP Communities

SNMP communities were introduced into SNMPv1 and retained in version 2c. Although the switch's software still supports communities, this is to provide backward compatibility with legacy management systems. Communities should not be used where a secure network is required. Instead, use the secure network features offered by SNMPv3.

An SNMP community is a pairing of an SNMP agent with a set of SNMP application entities. Communities are the main configuration item in the switch's implementation of SNMPv1 and v2, and are defined in terms of a list of IP addresses which define the SNMP application entities (trap hosts and management stations) in the community.

Important community names act as passwords and provide minimal authentication. Any SNMP application entity that knows a community name can read the value of any instance of any object in the MIB implemented in the switch. Any SNMP application entity that knows the name of a community with write access can change the value of any instance of any object in the MIB implemented in the switch, possibly affecting the operation of the switch. For this reason, take care with the security of community names.

When a trap is generated by the SNMP agent it is forwarded to all trap hosts in all communities. The community name and manager addresses are used to provide trivial authentication. An incoming SNMP message is deemed authentic if it contains a valid community name and originated from an IP address defined as a management station for that community.

When a community is disabled, the SNMP agent behaves as if the community does not exist and generates authentication failure traps for messages directed to the disabled community.

The SNMP agent does not support a default community called “public” with read-only access, traps disabled and open access as mandated in RFC 1812, as this is a security hole open for users who wish to use the switch with minimal modification to the default configuration. The default configuration of the switch has no defined communities. Communities must be explicitly created.

SNMP authentication (for SNMPv1 and v2) is a mechanism whereby an SNMP message is declared to be authentic, that is from an SNMP application entity actually in the community to which the message purports to belong. The mechanism may be trivial or secure. The only form of SNMP authentication implemented by the switch’s SNMP agent is trivial authentication. The authentication failure trap may be generated as a result of the failure to authentication an SNMP message.

Switch interfaces can be enabled or disabled via SNMP by setting the ifAdminStatus object in the ifTable of MIB-II MIB to ‘Up(1)’ or ‘Down(2)’ for the corresponding ifIndex. If it is not possible to change the status of a particular interface the switch returns an SNMP error message.

The switch’s implementation of the ifOperStatus object in the ifTable of MIB-II MIB supports two additional values—”Unknown(4)” and “Dormant(5)” (e.g. an inactive dial-on-demand interface).

Caution

An unauthorized person with knowledge of the appropriate SNMP community name could bring an interface up or down. Community names act as passwords for the SNMP protocol. When creating an SNMP community with write access, take care to select a secure community name and to ensure that only authorized personnel know it.

An SNMP MIB view is a subset of objects in the MIB that pertain to a particular network element. For example, the MIB view of a hub would be the objects relevant to management of the hub, and would not include IP routing table objects, for example. The switch’s SNMP agent does not allow the construction of MIB views. The switch supports all relevant objects from all MIBs that it implements.

Note that the switch’s standard set and show commands can also be used to access objects in the MIBs supported by the switch.

Defining management stations within communities

You can add management stations to a community either individually, by entering just its IP address, or you can enter a range of management stations by entering an IP address that ends with a ‘/’ character followed by a number between 1 and 32. The number that follows the ‘/’ character operates as an address mask to define a range of addresses for the management stations. The following example shows how to allocate a band of three binary addresses to a portion of the subnet 146.15.1.X

Example

In this example we make provision for up to 8 possible management stations within a community called “admin”.

Step 1:

Decide on the number of management stations that you want to assign to a particular subnet, then decide how many binary digits are required to define this number of addresses. In this case we need up to 8 management stations, so we will assign 3 binary digits (3 binary digits can provide 8 different values). To assign the last 3 binary digits for management stations, we assign a prefix that is a count of all binary digits in the address minus those to be assigned as management stations. In this case the prefix is 29; this being the number of binary digits in an IP address (32) minus the number of digits assigned to the management stations (3).

Step 2:

The method used in this step depends on whether or not the community already exists.

- If the community called “admin” does not exist, create a new community called “admin” and allocate a three binary digit block of addresses to the address subnet 146.15.1.X.
- If the community called “admin” already exists, allocate a three binary digit block of addresses to an existing community called “admin” with the address subnet 146.15.1.X.

For security reasons, the common management prefix should be larger than the IP subnet. This prevents stations on one subnet from being considered valid management stations on a different subnet.

Configuration Example (SNMPv1 and v2)

This example shows how to configure the switch’s SNMP agent. Two network management stations have been set up on a large network. The central NMS (IP address 192.168.11.5) monitors devices on the network and uses SNMP set messages to manage devices on the network. Trap messages are sent to this management station. The regional network management station (IP addresses 192.168.16.1) is used just to monitor devices on the network by using SNMP get messages. Link traps are enabled for all interfaces on this particular switch.

IP and VLANs must be correctly configured in order to access the SNMP agent in the switch. This is because the IP module handles both the TCP transport functions, and the UDP functions that enable datagrams to transport SNMP messages. See **Chapter 25, IP Addressing and Protocol Commands** for commands that enable and configure IP.

To configure SNMP

Step 1: Enable the SNMP agent.

Enable the SNMP agent and enable the generation of authenticate failure traps to monitor unauthorized SNMP access. SNMP is enabled by default in AlliedWare Plus.

```
awplus(config)# snmp-server enable trap auth
```

Step 2: Create a community with write access for the central NMS.

Create a write access community called “example1rw” for use by the central network management station at 192.168.11.5 Use an ACL to give the central NMS SNMP access to the switch using that community name.

```
awplus(config)# access-list 66 permit 192.168.11.5
awplus(config)# snmp-server community example1rw rw 66
```

Care must be taken with the security of community names. Do not use the names “private” or “public” in your network because they are too obvious. Community names act as passwords and provide only trivial authentication. Any SNMP application entity that knows a community name can read the value of any instance of any object in the MIB implemented in the switch. Any SNMP application entity that knows the name of a community with write access can change the value of any instance of any object in the MIB implemented in the switch, possibly affecting the operation of the switch.

SNMP V1 or V2c provide very minimal security. If security is a concern, you should use SNMPv3.

Step 3: Create a community with read-only access for the regional NMS.

Create a read-only access community called “example2ro” for use by the regional network management station at 192.168.16.1. Use an ACL to give the regional NMS SNMP access to the switch using that community name.

```
awplus(config)# access-list 67 permit 192.168.16.1
awplus(config)# snmp-server community example2ro ro 67
```

Step 4: Enable link traps.

Enable link traps for the desired interfaces. In this example, the NSMs are in VLAN 2 and VLAN 3 and other ports are in VLAN 1 for simplicity.

```
awplus(config)# interface vlan1-3
awplus(config-if)# snmp trap link-status
```

Note that link traps on VLANs are sent when the last port in the VLAN goes down. You will only see a trap for a VLAN if the trap host is in a different VLAN.

You can also enable link traps on channel groups and switch ports. For example, to enable traps on a range of switch ports:

```
awplus(config)# int port1.0.4-1.0.6
awplus(config-if)# snmp trap link-status
```

You can also enable link traps on channel groups and switch ports. For example, to enable traps on a range of switch ports:

Step 5: Configure trap hosts.

Specify the IP address or addresses that the traps will get sent to. In this example, traps will be sent to both NMSes.

```
awplus(config)# snmp-server host 192.168.11.5 version 2c
                example1rw
awplus(config)# snmp-server host 192.168.16.1 version 2c
                example2ro
```

Step 6: Check the configuration.

Check that the current configuration of the SNMP communities matches the desired configuration:

```
awplus# show snmp-server
awplus# show snmp-server community
awplus# show run snmp
```

This is the output of the **show snmp-server community** command for this example:

```
SNMP community information:
  Community Name ........... example1rw
    Access ................. Read-write
    View ................... none
  Community Name ........... example2ro
    Access ................. Read-only
    View ................... none
```

This is the output of the **show run snmp** command for this example:

```
no snmp-server ip
snmp-server enable trap auth
snmp-server community example1rw rw 66
snmp-server community example2ro 67
snmp-server host 192.168.1.2 version 2c example1rw
snmp-server host 192.168.2.2 version 2c example2ro
!
```

Check that the interface link up/down traps have been correctly configured:

```
awplus# show interface vlan1-3
```

This is the output of the **show interface** command for this example:

```
Interface vlan1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is VLAN, address is 0009.41fd.c029
  index 201 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Sending (suppressed after 20 traps in 60 sec)
  Bandwidth 1g
    input packets 4061, bytes 277043, dropped 0, multicast   packets 3690
    output packets 190, bytes 18123, multicast packets 0 broadcast packets 0
Interface vlan2
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0009.41fd.c029
  IPv4 address 192.168.11.50/24 broadcast 192.168.11.255
  index 202 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  SNMP link-status traps: Sending (suppressed after 20 traps in 60 sec)
  Bandwidth 1g
    input packets 568, bytes 42309, dropped 0, multicast packets 0
    output packets 183, bytes 18078, multicast packets 0 broadcast packets 0
Interface vlan3
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0009.41fd.c029
  IPv4 address 192.168.16.50/24 broadcast 192.168.16.255
  index 203 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  SNMP link-status traps: Sending (suppressed after 20 traps in 60 sec)
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
```

SNMPv3

SNMPv3 is the third version of the Simple Network Management Protocol. The architecture comprises the following:

- entities that may be either managers, agents, or both
- a management information base (MIB)
- a transport protocol

At least one manager node runs the SNMP management software in every configuration. Managed devices such as routers, servers, and workstations are equipped with an agent software module. The agent provides access to local objects in the MIB that reflect activity and resources at the node. The agent also responds to manager commands to retrieve values from, and set values in the MIB.

SNMP MIB Views for SNMPv3

An SNMP MIB view is a arbitrary subset of objects in the MIB. Objects in the view may be from any part of the object name space, and not necessarily the same sub-tree.

SNMP Groups

Groups were introduced as part of SNMPv3. They are the means by which users are assigned their views and access control policy. Once a group has been created, users can be added to them. In practice a number of groups would be created, each with varying views and access security requirements. Users would then be added to their most appropriate groups. Each Group name and Security Level pair must be unique within a switch.

SNMP Users

Users were introduced as part of SNMPv3. From a system perspective a user is represented as an entity stored in a table that defines the access and authentication criteria to be applied to access or modify the SNMP MIB data.

Note SNMP **Target Addresses** and **Target Params** in SNMPv3 are not currently supported in Alliedware Plus software.

Configuration Example (SNMPv3)

This example shows how to configure the switch's SNMP agent. Two network management stations have been set up on a large network. The central NMS (IP address 192.168.11.5) monitors devices on the network and uses SNMP set messages to manage devices on the network. Trap messages are sent to this management station.

The IP module must be enabled and correctly configured in order to access the SNMP agent in the switch, since the IP module handles the UDP datagrams used to transport SNMP messages.

To configure SNMP

Step 1: Enable the SNMP agent.

Enable the SNMP agent and enable the generation of authenticate failure traps to monitor unauthorized SNMP access. SNMP is enabled by default in AlliedWare Plus.

Step 2: Add SNMP views.

You can specify views using their OID or the predefined MIB name.

```
awplus(config)# snmp-server view atmib 1.3.6.1.2.14
included

awplus(config)# snmp-server view atmib alliedtelesis
included
```

Step 3: Add SNMP group.

```
awplus(config)# snmp-server group ord-user noauth read
atmib

awplus(config)# snmp-server group admin-user auth read
atmib write atmib notify atmi
```

Step 4: Add SNMP users.

Add users to the groups by using commands such as:

```
awplus(config)# snmp-server user ken admin-user auth md5
mercury
```

Using SNMP to Manage Files and Software

The Allied Telesis Enterprise MIB (**Chapter 68, SNMP MIBs**) includes objects for managing files and software on the switch. This section includes procedures for using MIB objects on the switch to perform some common tasks, via an SNMP management application:

- **"Copy a File to or from a TFTP Server" on page 66.20**
- **"Upgrade Software and Configuration Files" on page 66.22**

For more details about the Allied Telesis Enterprise MIB and public MIBs on the switch, see **Chapter 68, SNMP MIBs**.

Copy a File to or from a TFTP Server

Use this procedure to copy a file (for example, a software version file) to the switch from a TFTP server, or to copy a file (for example, a configuration file) from the switch to a TFTP server. The MIB objects in this procedure reside in the module atFilev2 { modules 600 }, with object ID 1.3.6.1.4.1.207.8.4.4.4.600. For detailed descriptions of the MIB objects used in this procedure, and other file management MIB objects, see **"AT-FILEv2-MIB" on page 68.32**. Other MIB objects can be used in a similar way for moving and deleting files on the switch.

Table 66-5: Procedure for copying a file to or from a device using a TFTP server

	Do this ...	By setting or reading this MIB object ...	Whose object ID is ...	To this value ...
1.	If the source device is part of a stack, set the stack ID. For a standalone switch, keep the default value, 1.	atFilev2SourceStackId	{ atFilev2Operation 1 }	*<stack-id>*
2.	If the destination device is part of a stack, set the stack ID.	atFilev2DestinationStackId	{ atFilev2Operation 4 }	*<stack-id>*
3.	Set the source device.	atFilev2SourceDevice	{ atFilev2Operation 2 }	4 (TFTP) or 1 (Flash)
4.	Set the destination device.	atFilev2DestinationDevice	{ atFilev2Operation 5 }	4 (TFTP) or 1 (Flash)
5.	Set the source filename. Include the path (if any) but not the device.	atFilev2SourceFileName	{ atFilev2Operation 3 }	*<source-filename>* e.g. /awp/config/admin.cfg
6.	Set the destination filename. Include the path (if any) but not the device.	atFilev2DestinationFileName	{ atFilev2Operation 6 }	*<dest-filename>* e.g. /config/admin.cfg

Table 66-5: Procedure for copying a file to or from a device using a TFTP server

	Do this ...	By setting or reading this MIB object ...	Whose object ID is ...	To this value ...
7.	Set the IP address of the TFTP server.	atFilev2TftpIPAddr	{ atFilev2Tftp_4 1 }	*<ip-addr>*
8.	Check that no other transfer is in progress, and that the required parameters have been set.	atFilev2CopyBegin	{ atFilev2Operation 7 }	Read: idle
9.	Start the file transfer.	atFilev2CopyBegin	{ atFilev2Operation 7 }	Set: 1
10	Monitor file transfer progress.	atFilev2CopyBegin	{ atFilev2Operation 7 }	Read: In progress: copying *<src>* --> *<dst>* *or* Success: copy *<src>* --> *<dst>* success *or* Failure: copy *<src>* --> *<dst>* failure: *<err-msg>*

Upgrade Software and Configuration Files

Use this procedure to upgrade to a new software version and boot configuration file. For detailed descriptions of the MIB objects used in this procedure, and other MIB objects for managing software installation and configuration files, see **"AT-SETUP-MIB" on page 68.57**.

Table 66-6: Procedure for upgrading to a new software version and boot configuration

	Do this ...	By reading or setting this MIB object ...	Whose object ID is ...	To this value ...
1.	Check that you have enough flash memory for the currently running software file, the new software version file, and any configuration scripts required.			
2.	Check the version and name of the software currently running.	currSoftVersion currSoftName	1.3.6.1.4.1.207.8.4.4.4.500.2.1.1 1.3.6.1.4.1.207.8.4.4.4.500.2.1.2	Read: <*software-name*> <*software-version*>
3.	If you do not already have the currently running software as a software version file in flash, save the currently running software with a file name to the flash root.	currSoftSaveToFile	1.3.6.1.4.1.207.8.4.4.4.500.2.1.4	Set: <*backup-filename.rel*>
4.	Check that the file saved successfully. (The most common failures result from lack of flash memory space.)	currSoftSaveStatus	1.3.6.1.4.1.207.8.4.4.4.500.2.1.5	Read: ■ 1 (idle) - there is no release file save operation in progress ■ 2 (success) - the last release file save operation completed successfully ■ 3 (failure) - the last release file save operation failed ■ 4 (saving) - a release file save operation is currently in progress
5.	Copy the new software version file to flash memory on the device	See **Table 66-5**.		
6.	Set the new release file to be the current release that the device will install and run the next time it restarts. Include the path.	nextBootPath	1.3.6.1.4.1.207.8.4.4.4.500.2.2.2	Set: <*next-filename*> e.g.: `flash:/release.rel`
7.	Check the version of release file set to install next.	nextBootVersion	1.3.6.1.4.1.207.8.4.4.4.500.2.2.1	Read: <*software-version*>

Table 66-6: Procedure for upgrading to a new software version and boot configuration(cont.)

	Do this ...	By reading or setting this MIB object ...	Whose object ID is ...	To this value ...
8.	Set the previous release file to be the backup release that the device will install and run if the device fails to boot successfully with the new release file. Include the path.	bckpPath	1.3.6.1.4.1.207.8.4.4.4.500.2.3.2	Set: *<backup-filename>* e.g.: `flash:/release.rel`
9.	Check the version of backup release file.	bckpVersion	1.3.6.1.4.1.207.8.4.4.4.500.2.3.1	Read: *<software-version>*
10.	If necessary, copy a configuration file to the device (**Table 66-5**), or save the current running configuration to a file in the root directory of flash. To save the running configuration, specify the filename, but not a device or path.	See **Table 66-5**. or runCnfgSaveAs	1.3.6.1.4.1.207.8.4.4.4.500.3.1.1	Set: *<filename.cfg>* e.g.: myconfig.cfg
11.	Check and if necessary set the file the device will use for configuration when it restarts. Include the full path.	bootCnfgPath	1.3.6.1.4.1.207.8.4.4.4.500.3.2.1	Read/set: *<filename.cfg>* e.g.: flash:/myconfig.cfg
12.	Check that a boot configuration file matching the boot configuration path exists.	bootCnfgExists	1.3.6.1.4.1.207.8.4.4.4.500.3.2.2	Read: TRUE (1) or FALSE (2)
13.	Check that the default configuration file flash:/default.cfg exists.	dfltCnfgExists	1.3.6.1.4.1.207.8.4.4.4.500.3.3.2	Read: TRUE (1) or FALSE (2)
14.	Restart the device.	restartDevice	1.3.6.1.4.1.207.8.4.4.4.500.1	1

Chapter 67: SNMP Commands

Command List 67.2
debug snmp 67.2
show counter snmp-server 67.4
show debugging snmp 67.8
show running-config snmp 67.8
show snmp-server 67.9
show snmp-server community 67.9
show snmp-server group 67.10
show snmp-server user 67.10
show snmp-server view 67.11
snmp trap link-status 67.12
snmp trap link-status suppress 67.13
snmp-server 67.15
snmp-server community 67.16
snmp-server contact 67.17
snmp-server enable trap 67.18
snmp-server engineID local 67.20
snmp-server engineID local reset 67.22
snmp-server group 67.23
snmp-server host 67.24
snmp-server location 67.26
snmp-server source-interface 67.27
snmp-server startup-trap-delay 67.28
snmp-server user 67.29
snmp-server view 67.31
undebug snmp 67.32

Command List

This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see **Chapter 66, SNMP Introduction**, and **Chapter 68, SNMP MIBs**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

debug snmp

This command enables SNMP debugging.

The **no** variant of this command disables SNMP debugging.

Syntax

```
debug snmp [all|detail|error-string|process|receive|send|xdump]
no debug snmp [all|detail|error-string|process|receive|send|xdump]
```

Parameter	Description
`all`	Enable or disable the display of all SNMP debugging information.
`detail`	Enable or disable the display of detailed SNMP debugging information.
`error-string`	Enable or disable the display of debugging information for SNMP error strings.
`process`	Enable or disable the display of debugging information for processed SNMP packets.
`receive`	Enable or disable the display of debugging information for received SNMP packets.
`send`	Enable or disable the display of debugging information for sent SNMP packets.
`xdump`	Enable or disable the display of hexadecimal dump debugging information for SNMP packets.

Mode Privileged Exec and Global Configuration

Example To start SNMP debugging, use the command:

```
awplus# debug snmp
```

To start SNMP debugging, showing detailed SNMP debugging information, use the command:

```
awplus# debug snmp detail
```

To start SNMP debugging, showing all SNMP debugging information, use the command:

```
awplus# debug snmp all
```

Related Commands

show debugging snmp
terminal monitor
undebug snmp

show counter snmp-server

This command displays counters for SNMP messages received by the SNMP agent.

Syntax `show counter snmp-server`

Mode User Exec and Privileged Exec

Example To display the counters for the SNMP agent, use the command:

```
awplus# show counter snmp-server
```

Output **Figure 67-1: Example output from the show counter snmp-server command**

```
SNMP-SERVER counters
inPkts                  ......... 11
inBadVersions           ......... 0
inBadCommunityNames     ......... 0
inBadCommunityUses      ......... 0
inASNParseErrs          ......... 0
inTooBigs               ......... 0
inNoSuchNames           ......... 0
inBadValues             ......... 0
inReadOnlys             ......... 0
inGenErrs               ......... 0
inTotalReqVars          ......... 9
inTotalSetVars          ......... 0
inGetRequests           ......... 2
inGetNexts              ......... 9
inSetRequests           ......... 0
inGetResponses          ......... 0
inTraps                 ......... 0
outPkts                 ......... 11
outTooBigs              ......... 0
outNoSuchNames          ......... 2
outBadValues            ......... 0
outGenErrs              ......... 0
outGetRequests          ......... 0
outGetNexts             ......... 0
outSetRequests          ......... 0
outGetResponses         ......... 11
outTraps                ......... 0
UnSupportedSecLevels    ......... 0
NotInTimeWindows        ......... 0
UnknownUserNames        ......... 0
UnknownEngineIDs        ......... 0
WrongDigest             ......... 0
DecryptionErrors        ......... 0
UnknownSecModels        ......... 0
InvalidMsgs             ......... 0
UnknownPDUHandlers      ......... 0
```

Table 67-1: Parameters in the output of show counter snmp-server

Parameter	Meaning
inPkts	The total number of SNMP messages received by the SNMP agent.
inBadVersions	The number of messages received by the SNMP agent for an unsupported SNMP version. It drops these messages.The SNMP agent on your device supports versions 1, 2C, and 3.
inBadCommunityNames	The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.
inBadCommunityUses	The number of messages received by the SNMP agent where the requested SNMP operation is not permitted from SNMP managers using the SNMP community named in the message.
inASNParseErrs	The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.
inTooBigs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inNoSuchNames	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inBadValues	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inReadOnlys	The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error-status field. This indicates that there is an incorrect implementations of the SNMP.
inGenErrs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.
inTotalReqVars	The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.
inTotalSetVars	The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.
inGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.
inGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.
inSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.

Table 67-1: Parameters in the output of show counter snmp-server (cont.)

Parameter	Meaning
inGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.
inTraps	The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.
outPkts	The number of SNMP Messages that the SNMP agent has sent.
outTooBigs	The number of SNMP PDUs that the SNMP agent has generated with the value ‘tooBig’ in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outNoSuchNames	The number of SNMP PDUs that the SNMP agent has generated with the value `noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outBadValues	The number of SNMP PDUs that the SNMP agent has generated with the value ‘badValue’ in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGenErrs	The number of SNMP PDUs that the SNMP agent has generated with the value ‘genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has generated.
outGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has generated.
outSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has generated.
outGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has generated.
outTraps	The number of SNMP Trap PDUs that the SNMP agent has generated.
UnSupportedSecLevels	The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent.
NotInTimeWindows	The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent’s window.
UnknownUserNames	The number of received packets that the SNMP agent has dropped because they referenced an unknown user.
UnknownEngineIDs	The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.
WrongDigest	The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.

Table 67-1: Parameters in the output of show counter snmp-server (cont.)

Parameter	Meaning
DecryptionErrors	The number of received packets that the SNMP agent has dropped because they could not be decrypted.
UnknownSecModels	The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.
InvalidMsgs	The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.
UnknownPDUHandlers	The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.

Related Commands show snmp-server

show debugging snmp

This command displays whether SNMP debugging is enabled or disabled.

Syntax `show debugging snmp`

Mode User Exec and Privileged Exec

Example To display the status of SNMP debugging, use the command:

```
awplus# show debugging snmp
```

Output **Figure 67-2: Example output from the show debugging snmp command**

```
Snmp (SMUX) debugging status:
  Snmp debugging is on
```

Related Commands debug snmp

show running-config snmp

This command displays the current configuration of SNMP on your device.

Syntax `show running-config snmp`

Mode Privileged Exec

Example To display the current configuration of SNMP on your device, use the command:

```
awplus# show running-config snmp
```

Output **Figure 67-3: Example output from the show running-config snmp command**

```
snmp-server contact AlliedTelesis
snmp-server location Philippines
snmp-server group grou1 auth read view1 write view1 notify view1
snmp-server view view1 1 included
snmp-server community public
snmp-server user user1 group1 auth md5 password priv des
password
```

Related Commands show snmp-server

show snmp-server

This command displays the status and current configuration of the SNMP server.

Syntax `show snmp-server`

Mode Privileged Exec

Example To display the status of the SNMP server, use the command:

```
awplus# show snmp-server
```

Output **Figure 67-4: Example output from the show snmp-server command**

```
SNMP Server ......................... Enabled
IP Protocol ......................... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ............ 0x80001f888021338e4747b8e607
```

Related Commands
debug snmp
show counter snmp-server
snmp-server
snmp-server engineID local
snmp-server engineID local reset

show snmp-server community

This command displays the SNMP server communities configured on the device. SNMP communities are specific to v1 and v2c.

Syntax `show snmp-server community`

Mode Privileged Exec

Example To display the SNMP server communities, use the command:

```
awplus# show snmp-server community
```

Output **Figure 67-5: Example output from the show snmp-server community command**

```
SNMP community information:
  Community Name ........... public
    Access ................. Read-only
    View ................... none
```

Related Commands
show snmp-server
snmp-server community

show snmp-server group

This command displays information about SNMP server groups. This command is used with SNMP version 3 only.

Syntax `show snmp-server group`

Mode Privileged Exec

Example To display the SNMP groups configured on the device, use the command:

```
awplus# show snmp-server group
```

Output **Figure 67-6: Example output from the show snmp-server group command**

```
SNMP group information:
  Group name ..... guireadgroup
    Security Level ..... priv
    Read View ..... guiview
    Write View ..... none
    Notify View ..... none

  Group name ..... guiwritegroup
    Security Level ..... priv
    Read View ..... none
    Write View ..... guiview
    Notify View ..... none
```

Related Commands **show snmp-server**
snmp-server group

show snmp-server user

This command displays the SNMP server users and is used with SNMP version 3 only.

Syntax `show snmp-server user`

Mode Privileged Exec

Example To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

Output **Figure 67-7: Example output from the show snmp-server user command**

```
Name            Group name        Auth       Privacy
-------         -------------     -------    ----------
freddy          guireadgroup      none       none
```

Related Commands **show snmp-server**
snmp-server user

show snmp-server view

This command displays the SNMP server views and is used with SNMP version 3 only.

Syntax `show snmp-server view`

Mode Privileged Exec

Example To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

Output **Figure 67-8: Example output from the show snmp-server view command**

```
SNMP view information:
  View Name ............... view1
    OID ..................... 1
    Type .................... included
```

Related Commands **show snmp-server**
snmp-server view

snmp trap link-status

Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

Syntax

```
snmp trap link-status
no snmp trap link-status
```

Default By default, link status notifications are disabled.

Mode Interface Configuration

Usage The link status notifications can be enabled for the following interface types:

- device port (e.g. port 1.0.1)
- VLAN (e.g. vlan2)
- static and dynamic link aggregation (e.g. sa2, po2)

To specify where notifications are sent, use the **snmp-server host** command on page 67.24. To configure the device globally to send other notifications, use the **snmp-server enable trap** command on page 67.18.

Examples To enable SNMP to send link status notifications for ports 1.0.2 to 1.0.6, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status
```

Related Commands

show interface
snmp trap link-status suppress
snmp-server enable trap
snmp-server host

snmp trap link-status suppress

Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the **no** variant of this command to disable the suppression of link status notifications for the ports.

Syntax

```
snmp trap link-status suppress {time {<1-60>|default}|
   threshold {<1-20>|default}}

no snmp trap link-status suppress
```

Parameter	Description
`time`	Set the suppression timer for link status notifications.
<1-60>	The suppress time in seconds.
`default`	The default suppress time in seconds (60).
`threshold`	Set the suppression threshold for link status notifications. This is the number of link status notifications after which to suppress further notifications within the suppression timer interval.
<1-20>	The number of link status notifications.
`default`	The default number of link status notifications (20).

Default By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

Mode Interface Configuration

Usage An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface. If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

Examples To enable the suppression of link status notifications for ports 1.0.2 to 1.0.6 after 10 notifications have been sent in 40 seconds, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status suppress time 40
                   threshold 10
```

To disable the suppression link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status suppress
```

Related Commands **show interface**
snmp trap link-status

snmp-server

Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the **snmp-server enable trap** command on page 67.18.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax

```
snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]
```

Parameter	Description
ip	Enable or disable the SNMP agent for IPv4.
ipv6	Enable or disable the SNMP agent for IPv6.

Default By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

Mode Global Configuration

Examples To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

Related Commands

show snmp-server
show snmp-server community
show snmp-server user
snmp-server community
snmp-server contact
snmp-server enable trap
snmp-server engineID local
snmp-server group
snmp-server host
snmp-server location
snmp-server view

snmp-server community

This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read only. If view is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

Syntax

```
snmp-server community <community-name> {view <view-name>|ro|rw|
    <access-list>}
no snmp-server community <community-name> [{view <view-name>|<access-
    list>}]
```

Parameter	Description
`<community-name>`	Community name. The community name is a case sensitive string of up to 20 characters.
`view`	Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
`<view-name>`	View name. The view name is a string up to 20 characters long and is case sensitive.
`ro`	Read-only community.
`rw`	Read-write community.
`<access-list>`	*<1-99>* Access list number.

Mode Global Configuration

Example The following command creates an SNMP community called “public” with read only access to all MIB variables from any management station.

```
awplus# configure terminal
awplus(config)# snmp-server community public ro
```

The following command removes an SNMP community called “public”

```
awplus# configure terminal
awplus(config)# no snmp-server community public
```

Related Commands
show snmp-server
show snmp-server community
snmp-server view

snmp-server contact

This command sets the contact information for the system. The contact name is:

- displayed in the output of the **show system** command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

Syntax

```
snmp-server contact <contact-info>
no snmp-server contact
```

Parameter	Description
<contact-info>	The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the system contact information to "support@alliedtelesis.co.nz", use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact support@alliedtelesis.co.nz
```

Related Commands

show system
snmp-server location
snmp-server group

snmp-server enable trap

Use this command to enable the device to send the specified notifications (traps).

Note that the Environmental Monitoring traps are enabled by default. So you do not need to issue this command for the Environmental Monitoring traps since these are enabled by default. SNMP environmental monitoring traps defined in AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the sending of the specified notifications.

Syntax

```
snmp-server enable trap {[atmf][atmflink][atmfnode][atmfrr][auth]
    [dhcpsnooping] [epsr] [lldp] [loopprot] [mstp] [nsm]
    [power-inline] [rmon] [thrash-limit] [vcs]}

no snmp-server enable trap {[atmf][atmflink][atmfnode][atmfrr][auth]
    [dhcpsnooping] [epsr] [lldp] [loopprot] [mstp] [nsm]
    [power-inline] [rmon] [thrash-limit] [vcs]}
```

Parameter	Description
`atmf`	ATMF traps.
`atmflink`	ATMF Link traps.
`atmfnode`	ATMF Node traps.
`atmfrr`	ATMF Reboot Rolling traps.
`auth`	Authentication failure.
`dhcpsnooping`	DHCP snooping and ARP security traps. These notifications must also be set using the **ip dhcp snooping violation** command on page 56.22, and/or the **arp security violation** command on page 56.3.
`epsr`	EPSR traps.
`lldp`	Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the **lldp notifications** command on page 70.13, and/or the **lldp med-notifications** command on page 70.8.
`loopprot`	Loop Protection traps.
`mstp`	MSTP traps.
`nsm`	NSM traps.
`power-inline`	Power-inline traps (Power Ethernet MIB RFC 3621).
`rmon`	RMON traps.
`thrash-limit`	MAC address Thrash Limiting traps.
`vcs`	VCS traps.

Default By default, no notifications are generated.

Mode Global Configuration

Usage

This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the **snmp trap link-status** command.

To specify where notifications are sent, use the **snmp-server host** command.

Note that more than one trap can be configured with one command entry, and also note this command applied to notifications send by SNMP version 3.

Examples

To enable the device to send a notification if an atmf node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send PoE related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
```

To disable PoE traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable power-inline
```

To enable the device to send MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap thrash-limit
```

To disable the device from sending MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap thrash-limit
```

Related Commands

show snmp-server
show ip dhcp snooping
snmp trap link-status
snmp-server host

snmp-server engineID local

Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command. Note that the **snmp-server engineID local reset** command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

Syntax

```
snmp-server engineID local {<engine-id>|default}
no snmp-server engineID local
```

Parameter	Description
<engine-id>	Specify SNMPv3 Engine ID value, a string of up to 27 characters.
`default`	Set SNMPv3 engine ID to a system generated value by resetting the SNMPv3 engine, provided the current engine ID is user defined. If the current engine ID is system generated, use the **snmp-server engineID local reset** command to force the system to generate a new engine ID.

Mode Global Configuration

Usage All devices must have a unique engine ID which is permanently set unless it is configured by the user.

In a stacked environment, if the same engine ID was automatically generated for all members of the stack, conflicts would occur if the stack was dismantled. Therefore, each member of the stack will generate its own engine ID and the stack master's ID is used when transmitting SNMPv3 packets. Should a master failover occur, a different engine ID is transmitted. You can modify this behavior by manually assigning all stack members the same engine ID using the **snmp-server engineID local** command. However, should you decide to separate the stack and use the devices individually, you must remember to change or remove this configuration to prevent conflicts.

Example To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

Output The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server ......................... Enabled
IP Protocol ......................... IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server ......................... Enabled
IP Protocol ......................... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483
```

Validation Commands **show snmp-server**

Related Commands **snmp-server engineID local reset**
snmp-server group

snmp-server engineID local reset

Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the **snmp-server engineID local** command to set SNMPv3 engine ID to a system generated value.

Syntax `snmp-server engineID local reset`

Mode Global Configuration

Example To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

Validation Commands **show snmp-server**

Related Commands **snmp-server engineID local**

snmp-server group

This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

Syntax

```
snmp-server group <groupname> {auth|noauth|priv} [read <readname>|
    write <writename>|notify <notifyname>]

no snmp-server group <groupname> {auth|noauth|priv}
```

Parameter	Description
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`auth`	Authentication.
`noauth`	No authentication and no encryption.
`priv`	Authentication and encryption.
`read`	Configure read view.
<readname>	Read view name.
`write`	Configure write view.
<writename>	Write view name. The view name is a string up to 20 characters long and is case sensitive.
`notify`	Configure notify view.
<notifyname>	Notify view name. The view name is a string up to 20 characters long and is case sensitive.

Mode Global Configuration

Examples To add SNMP group, for ordinary users, user the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server group usergroup noauth read
                useraccess write useraccess
```

To delete SNMP group `usergroup`, use the following commands

```
awplus# configure terminal
awplus(config)# no snmp-server group usergroup noauth
```

Related Commands

snmp-server
show snmp-server
show snmp-server group
show snmp-server user

snmp-server host

This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6),
- inform or trap messages,
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

Syntax

```
snmp-server host {<ipv4-address>|<ipv6-address>} [traps] [version 1]
   <community-name>]

snmp-server host {<ipv4-address>|<ipv6-address>} [informs|traps]
   version 2c <community-name>

snmp-server host {<ipv4-address>|<ipv6-address>} [informs|traps]
   version 3 {auth|noauth|priv} <user-name>

no snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
   [version 1] <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>} [informs|traps]
   version 2c <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>} [informs|traps]
   version 3 {auth|noauth|priv} <user-name>
```

Parameter	Description
<ipv4-address>	IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.
<ipv6-address>	IPv6 trap host address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
informs	Send Inform messages to this host.
traps	Send Trap messages to this host (default).
version	SNMP version to use for notification messages. Default: version 1.
1	Use SNMPv1(default).
2c	Use SNMPv2c.
3	Use SNMPv3.
auth	Authentication.
noauth	No authentication.

Parameter(cont.)	Description(cont.)
`priv`	Encryption.
<community-name>	The SNMPv1 or SNMPv2c community name.
<user-name>	SNMPv3 user name.

Mode Global Configuration

Examples To configure the device to send generated traps to the IPv4 host destination `192.0.2.5` with the SNMPv2c community name *public*, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to the IPv6 host destination `2001:db8::8a2e:7334` with the SNMPv2c community name *private*, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host 2001:db8::8a2e:7334 version 2c
private
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name *public*, use the following command:

```
awplus# configure terminal
awplus(config)# no snmp-server host 192.0.2.5 version 2c public
```

Related Commands **snmp trap link-status**
snmp-server enable trap
snmp-server view

snmp-server location

This command sets the location of the system. The location is:

- displayed in the output of the **show system** command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

Syntax

```
snmp-server location <location-name>
no snmp-server location
```

Parameter	Description
<location-name>	The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

Related Commands

show snmp-server
show system
snmp-server contact

snmp-server source-interface

Use this command to specify the interface that SNMP traps or informs originate from. You cannot specify an interface that does not already have an IP address assigned to the interface.

Use the **no** variant of this command to reset to the default source interface that SNMP traps or informs originate from (the Egress interface as sent from by default).

Syntax

```
snmp-server source-interface {traps|informs} <interface-name>
no snmp-server source-interface {traps|informs}
```

Parameter	Description
`traps`	SNMP traps.
`informs`	SNMP informs.
<interface-name>	Interface name (with an IP address already assigned).

Default By default the source interface is the Egress interface where traps or informs were sent from.

Mode Global Configuration

Usage An SNMP trap or inform sent from an SNMP server has the notification IP address of the interface where it was sent from. Use this command to monitor notifications from an interface.

Example To set the interface that SNMP informs originate from to port 1.0.2 for inform packets, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs port1.0.2
```

To reset the interface to the default source interface (the Egress interface) that SNMP traps originate from for trap packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

Validation Commands **show running-config**

snmp-server startup-trap-delay

Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the **no** variant of this command to restore the default startup delay of 30 seconds.

Syntax

```
snmp-server startup-trap-delay <delay-time>

no snmp-server startup-trap-delay
```

Parameter	Description
<delay-time>	Specify an SNMP trap delay time in seconds in the range of **30 to 600** seconds.

Default The SNMP server trap delay time is 30 seconds. The **no** variant restores the default.

Mode Global Configuration

Example To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

Validation Commands **show snmp-server**

snmp-server user

Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

Syntax

```
snmp-server user <username> <groupname> [encrypted] [auth {md5|
    sha} <auth-password>] [priv {des|aes} <privacy-password>]

no snmp-server user <username>
```

Parameter	Description
<username>	User name. The user name is a string up to 20 characters long and is case sensitive.
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`encrypted`	Use the encrypted parameter when you want to enter encrypted passwords.
`auth`	Authentication protocol.
`md5`	MD5 Message Digest Algorithms.
`sha`	SHA Secure Hash Algorithm.
<auth-password>	Authentication password. The password is a string of 8 to 20 characters long and is case sensitive.
`priv`	Privacy protocol.
`des`	DES Data Encryption Standard.
`aes`	AES Advanced Encryption Standards.
<privacy-password>	Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.

Mode Global Configuration

Usage Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.
- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.

- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

Examples To add SNMP user `authuser` as a member of group `usergroup`, with authentication protocol `md5`, authentication password `Authpass`, privacy protocol `des` and privacy password `Privpass`, use the following commands

```
awplus# configure terminal
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv des Privpass
```

Validate the user is assigned to the group using the following command:

```
awplus#show snmp-server user
Name                Group name          Auth        Privacy
-------             -------------       -------     ----------
authuser            usergroup           md5         des
```

To enter existing SNMP user `authuser` with existing passwords as a member of group `newusergroup` with authentication protocol `md5` plus the encrypted authentication password `0x1c74b9c22118291b0ce0cd883f8dab6b74`, privacy protocol `des` plus the encrypted privacy password `0x0e0133db5453ebd03822b004eeacb6608f`, use the following commands

```
awplus# configure terminal
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5
0x1c74b9c22118291b0ce0cd883f8dab6b74 priv des
0x0e0133db5453ebd03822b004eeacb6608f
```

Note

Copy and paste the encrypted passwords from the **running-config** or the **startup-config** displayed, using the **show running-config** and **show startup-config** commands respectively, into the command line to avoid key stroke errors issuing this command.

Validate the user has been moved from the first group using the following command:

```
awplus#show snmp-server user
Name                Group name          Auth        Privacy
-------             -------------       -------     ----------
authuser            newusergroup        md5         des
```

To delete SNMP user `authuser`, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server user authuser
```

Related Commands **show snmp-server user**
snmp-server view

snmp-server view

Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager's access.

Note

The object identifier must be specified in a sequence of integers separated by decimal points.

The **no** variant of this command removes the specified view on the device. The view must already exist.

Syntax

```
snmp-server view <view-name> <mib-name> {included|excluded}
no snmp-server view <view-name>
```

Parameter	Description
<view-name>	SNMP server view name. The view name is a string up to 20 characters long and is case sensitive.
<mib-name>	Object identifier of the MIB.
`included`	Include this OID in the view.
`excluded`	Exclude this OID in the view.

Mode Global Configuration

Examples The following command creates a view called "loc" that includes the system location MIB sub-tree.

```
awplus(config)# snmp-server view loc 1.3.6.1.2.1.1.6.0 included
```

To remove the view "loc" use the following command

```
awplus(config)# no snmp-server view loc
```

Related Commands

show snmp-server view
snmp-server community

undebug snmp

This command applies the functionality of the no **debug snmp** command.

Chapter 68: SNMP MIBs

Introduction 68.2
About MIBs 68.2
About SNMP 68.2
Obtaining MIBs 68.2
Loading MIBs 68.3
Allied Telesis Enterprise MIB 68.5
AT-ALMMON-MIB 68.6
AT-ATMF-MIB 68.8
AT-BOARDS-MIB 68.13
AT-DHCPSN-MIB 68.17
AT-DNS-CLIENT-MIB 68.20
AT-ENVMONv2-MIB 68.21
AT-EPSRv2-MIB 68.29
AT-FILEv2-MIB 68.32
AT-IP-MIB 68.39
AT-LICENSE-MIB 68.41
AT-LOG-MIB 68.44
AT-LOOPPROTECT-MIB 68.46
AT-MIBVERSION-MIB 68.48
AT-NTP-MIB 68.49
AT-PRODUCTS-MIB 68.52
AT-RESOURCE-MIB 68.55
AT-SETUP-MIB 68.57
AT-SMI-MIB 68.66
AT-SYSINFO-MIB 68.68
AT-TRIGGER-MIB 68.73
AT-USER-MIB 68.75
AT-VCSTACK-MIB 68.77
Other Enterprise MIBs 68.82
Public MIBs 68.83

Introduction

This chapter describes the Management Information Bases (MIBs) and managed objects supported by the AlliedWare Plus™ Operating System. The following topics are covered:

- **"Allied Telesis Enterprise MIB" on page 68.5** describes the objects implemented in the Allied Telesis Enterprise MIB
- **"Public MIBs" on page 68.83** describes the public MIBs supported by the AlliedWare Plus™ Operating System, and any variations from the standard implementation.

About MIBs

A MIB is a collection of managed objects organized into a tree-like hierarchy of nodes in which the managed objects form the leaves. Within the tree, each node is identified by a non-negative integer identifier that is unique among the node's siblings. The address, or object identifier, of any node within the tree is expressed as a series of dot-delimited node identifiers that trace the path from the root of the tree to the node. For example, the object identifier for the sysDescr object is 1.3.6.1.2.1.1.1.

For more information about MIBs and the structure of management information, see **Chapter 66, SNMP Introduction**.

This chapter does not indicate which MIB objects are not-accessible (and therefore cannot be queried directly). Please consult the MIB files for that information.

About SNMP

A network management station (NMS) uses a protocol known as Simple Network Management Protocol (SNMP) to query or change the values of objects in the MIB of managed devices.

A managed device uses SNMP to respond to queries from an NMS, and to send unsolicited alerts (traps) to an NMS in response to events.

For more information about the Simple Network Management Protocol (SNMP), see **Chapter 66, SNMP Introduction**.

For information about configuring SNMP, see **Chapter 67, SNMP Commands**.

Obtaining MIBs

You can download MIBs from the following locations:

Download this MIB...	From this location...
Allied Telesis Enterprise MIB	The MIB files are available with the software files from the Support area at **www.alliedtelesis.com/support/software**
Public MIBs defined in RFCs	**www.rfc-editor.org/rfc.html**
IANAifType-MIB	**www.iana.org/assignments/ianaiftype-mib**

Loading MIBs

Individual MIBs define a portion of the total MIB for a device. For example, the MAU-MIB defines objects for managing IEEE 802.3 medium attachment units (MAUs), and forms a sub-tree under mib-2 with the object identifier snmpDot3MauMgt (1.3.6.1.2.1.26).

All the objects within a MIB are assigned object identifiers relative to a parent object. Most MIBs import the object identifier of the parent object, along with other object identifiers, textual conventions, macros and syntax types from the MIBs where they are defined. This creates dependencies between MIBs.

Some network management stations and MIB compilers will generate errors if you load a MIB that depends on another MIB that has not already been loaded. To avoid these errors, we recommend that you load MIBs in the following order:

1. RFC 1212
   RFC 1239
   RFC 2257
   RFC 3410

2. RFC1155-SMI (RFC 1155)
   SNMPv2-SMI (RFC 2578)
   SNMPv2-PDU (RFC 3416)

3. RFC1213-MIB (RFC 1213)
   RFC 1215
   SNMPv2-TC (RFC 2579)
   SNMPv2-CONF (RFC 2580)

4. IP-MIB (RFC 2011)
   TCP-MIB (RFC 2012)
   UDP-MIB (RFC 2013)
   IP-FORWARD-MIB (RFC 2096)
   SNMP-MPD-MIB (RFC 2572)
   RMON-MIB (RFC 2819)
   HCNUM-TC (RFC 2856)
   SNMP-FRAMEWORK-MIB (RFC 3411)
   SNMP-MPD-MIB (RFC 3412)
   SNMPv2-TM (RFC 3417)
   SNMPv2-MIB (RFC 3418)
   INET-ADDRESS-MIB (RFC 4001)
   IANAifType-MIB

5. IF-MIB (RFC 2863)
   SNMP-TARGET-MIB (RFC 3413)

6. SNMP-COMMUNITY-MIB (RFC 2576)
   EtherLike-MIB (RFC 3635)
   MAU-MIB (RFC 3636)
   BRIDGE-MIB (RFC 4188)
   DISMAN-PING-MIB (RFC 4560)

SNMP-NOTIFICATION-MIB (RFC 3413)
SNMP-PROXY-MIB (RFC 3413)

7. P-BRIDGE-MIB (RFC 2674)
   Q-BRIDGE-MIB (RFC 2674)
   RSTP-MIB (RFC 4318)
   LLDP-MIB
   LLDP-EXT-DOT1-MIB
   LLDP-EXT-DOT3-MIB
   LLDP-EXT-MED-MIB
   POE-MIB

8. AT-SMI-MIB

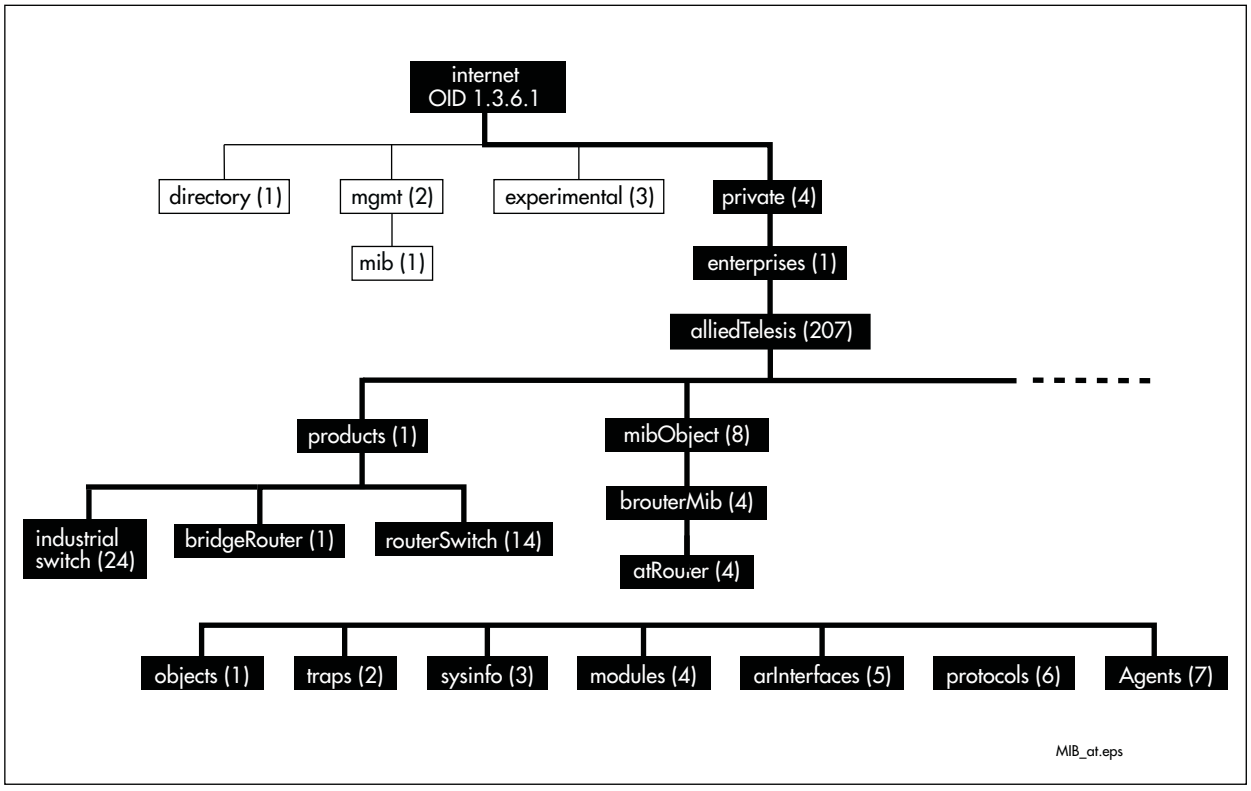
9. AT-BOARDS-MIB
   AT-PRODUCT-MIB
   AT-SETUP-MIB
   AT-SYSINFO-MIB
   AT-TRIGGER-MIB
   AT-VCSTACK-MIB
   AT-USER-MIB
   AT-RESOURCE-MIB
   AT-LICENSE-MIB
   AT-LOOPPROTECT-MIB
   AT-DNS-CLIENT--MIB
   AT-NTP-MIB
   AT-EPSRv2-MIB
   AT-FILEv2-MIB
   AT-LOG-MIB
   AT-IP-MIB
   AT-ENVMONv2-MIB
   AT-MIBVERSION-MIB
   AT-DHCPSN-MIB
   AT-ALMMON-MIB

Allied Telesis Enterprise MIB

The *Allied Telesis Enterprise MIB* defines a portion of the Management Information Base (MIB) for managing Allied Telesis products and features that are not supported by public MIBs. Objects defined in this MIB reside in the private(4) subtree and have the object identifier alliedTelesis ({ enterprises 207 }).

This document describes only those portions of the Allied Telesis Enterprise MIB supported by the AlliedWare Plus™ Operating System. **Figure 68-1** shows the structure of the Allied Telesis Enterprise MIB. Each component MIB is detailed in the following sections of this chapter.

Figure 68-1: The Allied Telesis Enterprise MIB sub-tree of the Internet-standard Management Information Base (MIB)



AT-ALMMON-MIB

AT-ALMMON-MIB defines objects for managing alarms **Table 68-1**. Objects in this group have the object identifier sysinfo ({ atRouter 3 }).

Table 68-1: .Objects defined by the atAlmMon MIB

Object / Object Identifier	Description
atAlmMon { atAlmMon 24 } (OID 1.3.6.1.4.1.207.8.4.4.3.26)	The AT Alarm Monitoring v2 MIB for managing and reporting device alarms.
atAlmMonActionTable { atAlmMon 1} (207.8.4.4.3.26.1)	Table of information defining alarm monitoring inputs and consequent actions (i.e. fault LED and relay outputs), indexed by: 1. atAlmMonActionStackMemberId 2. atAlmMonActionIndex
atAlmMonActionEntry { atAlmMonActionTable 1 } (207.8.4.4.3.26.1.1)	A description and configuration of what to do for a specific monitored alarm.
atAlmMonActionStackMemberId { atAlmMonActionEntry 1 } (207.8.4.4.3.26.1.1.1)	The index of the stack member of this alarm action. Read only.
atAlmMonActionIndex { atAlmMonActionEntry 2 } (207.8.4.4.3.26.1.1.2)	The numeric identifier of this alarm action. Read only.
atAlmMonAlarmType { alAlmMonActionEntry 3 } (207.8.4.4.3.26.1.1.3)	The type of alarm that this action monitors. Read only. Values can be: 1. alarmTypeInvalid (0) 2. externalPSU (1) 3. epsr (2) 4. contactInput (3) 5. portLinkDown (4) 6. loopDetect (5) 7. mainPse (6) 8. portPoeFailure (7) 9. temperature (8)
atAlmMonAlarmTypeSelection { atAlmMonActionEntry 4}	The 1-based index of the alarm of the particular type (as categorized by AlmMonAlarmType).
atAlmMonActionDescription { atAlmMonActionEntry 5}	The description of this alarm monitoring entry. Read only.
atAlmMonActionUseRelay1 { atAlmMonActionEntry 6 }	Indicates/controls whether or not this alarm monitor drives the first relay output. Read-write. Values can be: ■ Unused (1) ■ Used (2)
atAlmMonActionUseRelay2 { alAlmMonActionEntry 7 }	Indicates/controls whether or not this alarm monitor drives the second relay output. Read-write. Values can be: ■ Unused (1) ■ Used (2)

Object / Object Identifier		Description
	atAlmMonActionUseRelay3 { atAlmMonActionEntry 8 }	Indicates/controls whether or not this alarm monitor drives the third relay output. Read-write. Values can be: ■ Unused (1) ■ Used (2)
	atAlmMonActionUseFaultLed { alAlmMonActionEntry 9 }	Indicates/controls whether or not this alarm monitor drives the fault LED. Read-write. Values can be: ■ Unused (1) ■ Used (2)
	atAlmMonAbnormalState { atAlmMonActionEntry 10 }	Indicates/sets the abnormal (i.e., alarm active) state for a contact input. Only used for contactInput alarm monitors, ignored for all other types. Read-write. Values can be: ■ open (1) ■ closed (2)
	atAlmMonActionState { atAlmMonActionEntry 11 }	Indicates the current state of this alarm monitor. Read only. Values can be: ■ Inactive (1) ■ Active (2)

AT-ATMF-MIB

The ATMF-MIB defines objects for managing ATMF. Objects and triggers are shown diagrammatically in **Figure 68-2 on page 68.8** and **Figure 68-3 on page 68.9**. Objects in this group have the object identifier ATMF ({ modules 603 }). These are shown listed in **Figure 68-2 on page 68.10**.

Figure 68-2: The upper levels of the AT-ATMF MIB sub-tree

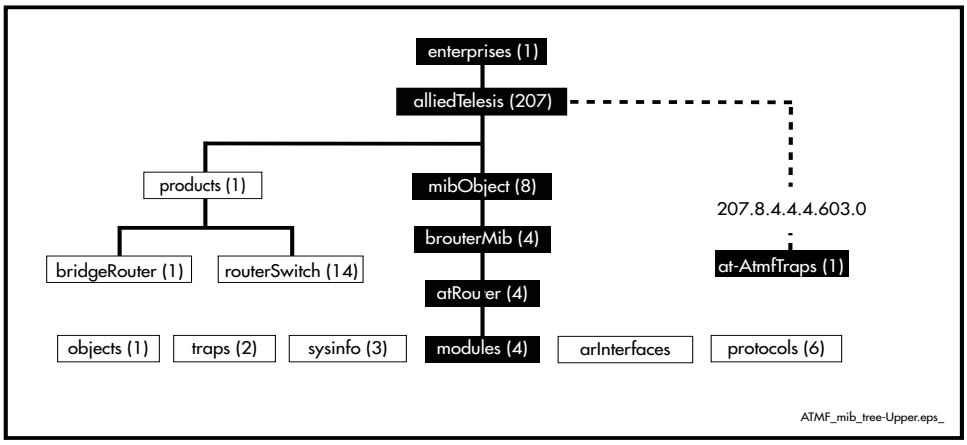


Figure 68-3: The Lower levels of the AT-ATMF MIB sub-tree

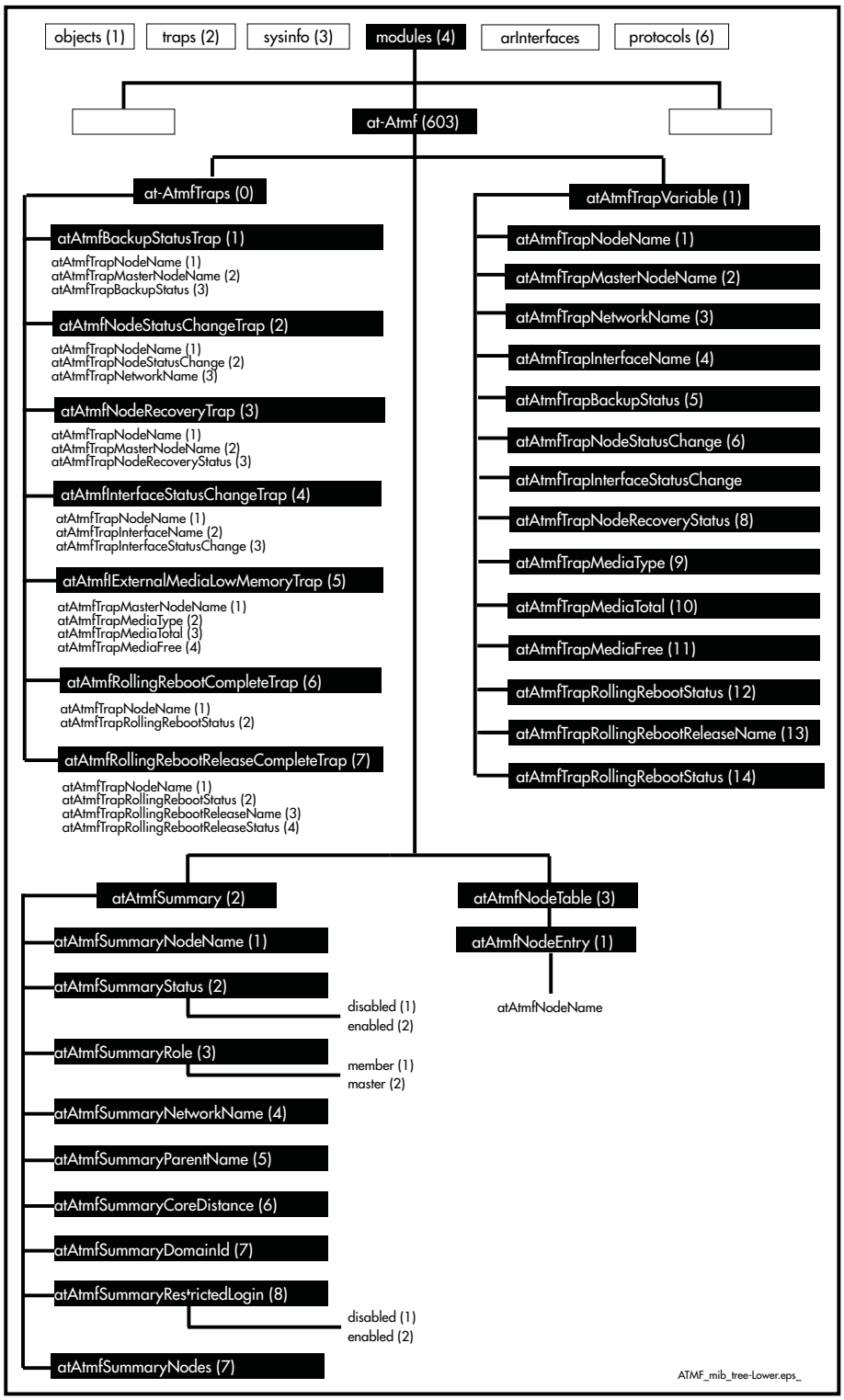


Table 68-2: AT-ATMF MIB Objects

Object	Object Identifier	Description
atmf	{ modules 603 } 1.3.6.1.4.1.207.8.4.4.4.603	Root of the Allied Telesis ATMF MIB under the private(4) node defined in RFC1155-SMI.
atAtmfTraps	{ atmf 0 } 207.8.4.4.4.603.0	Sub-tree of objects describing ATMF traps.
atAtmfBackup StatusTrap	atAtmfTraps 1	This trap is generated when an ATMF master attempts to backup a node's FLASH contents. It states whether the backup of an individual node, or all nodes, to a master node has passed or failed. Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapMasterNodeName 3. atAtmfTrapBackupStatus
atAtmfNode StatusChange Trap	atAtmfTraps 2	This trap is generated when an ATMF node joins or leaves the ATMF network. It states whether a node has <left| joined> an ATMF network. Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapNodeStatusChange 3. atAtmfTrapNetworkName
atAtmfNode RecoveryTrap	atAtmfTraps 3	This trap is generated when an attempt has been made to recover an ATMF node. It states whether an attempt to recover a node from the specified master has passed or failed. Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapMasterNodeName 3. atAtmfTrapNodeRecoveryStatus
atAtmfInterface StatusChangeTrap	atAtmfTraps 4	This trap is generated when an ATMF interface status change occurs. It states that an interface on a node has changed status to either blocking or forwarding. Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapInterfaceName 3. atAtmfTrapInterfaceStatusChange
atAtmfExternal MediaLowMemory Trap	atAtmfTraps 5	This trap is generated when the available external storage on the ATMF master node falls below a nominated threshold. It states that the external USB or SD card storage on a master node has fallen below the designated threshold and specifies the total available memory <xxx MB> and the total free memory <xxx MB>. Its objects are: 1. atAtmfTrapMasterNodeName 2. atAtmfTrapMediaType 3. atAtmfTrapMediaTotal 4. atAtmfTrapMediaFree
atAtmfRolling RebootComplete Trap	atAtmfTraps 6	This trap is generated when the ATMF rolling reboot process has finished on a particular ATMF node. Nominally, it states that the ATMF rolling reboot, executed against the specified node, has returned a reboot status of either failed or passed. Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapRollingRebootStatus

Table 68-2: AT-ATMF MIB Objects(cont.)

Object	Object Identifier	Description
atAtmfRolling RebootRelease CompleteTrap	atAtmfTraps 7	This trap is generated when the ATMF rolling reboot process attempts to push a new software release to a specified ATMF node. Nominally, it states that the ATMF rolling reboot release process, executed from the specified node has returned a reboot status of either failed or passed, the name of the attempted release file and the release status of either "failed" or "passed". Its objects are: 1. atAtmfTrapNodeName 2. atAtmfTrapRollingRebootStatus 3. atAtmfTrapRollingRebootReleaseName 4. atAtmfTrapRollingRebootReleaseStatus
atAtmfTrapVariable	atmf 1	Sub-tree of objects describing ATMF traps.
atAtmfTrapNode Name	atAtmfTrapVariable 1	The ATMF trap node name.
atAtmfTrapMaster NodeName	atAtmfTrapVariable 2	The ATMF trap master node name.
atAtmfTrapNetwork Name	atAtmfTrapVariable 3	The ATMF trap network name.
atAtmfTrapInterface Name	atAtmfTrapVariable 4	The ATMF interface name, "Trap".
atAtmfTrapBackup Status	atAtmfTrapVariable 5	The status of the last trap backup attempt on either a specified ATMF node or all nodes in the ATMF network. Its objects are: 1. failed(1) 2. passed(2)
atAtmfTrapNode StatusChange	atAtmfTrapVariable 6	An ATMF trap node has changed its status in the ATMF network. Its objects are: 1. left(1) 2. joined(2)
AtmfTrapInterface StatusChange	atAtmfTrapVariable 7	An ATMFtrap interface has changed its status. Its objects are: 1. blocking(1) 2. forwarding(2)
atAtmfTrapNode RecoveryStatus	atAtmfTrapVariable 8	The status of the last recovery attempt. Its objects are: 1. failed(1) 2. passed(2)
atAtmfTrapMedia Type	atAtmfTrapVariable 9	The media type resident on the ATMF node - USB or SD.
atAtmfTrapMedia Total	atAtmfTrapVariable 10	The total memory available on the resident media, in MB.
atAtmfTrapMedia Free	atAtmfTrapVariable 11	The free memory available on the resident media, in MB. Each node has a maximum flash of 64MB.
atAtmfTrapRolling RebootStatus	atAtmfTrapVariable 12	The status of the last rolling reboot for a node. Its objects are: 1. failed(1) 2. passed(2)
atAtmfTrapRolling RebootRelease Name	atAtmfTrapVariable 13	The name of the last rolling reboot release.

Table 68-2: AT-ATMF MIB Objects(cont.)

Object	Object Identifier	Description
atAtmfTrapRollingRebootReleaseStatus	atAtmfTrapVariable 14	The release update status of the last rolling reboot for a node. Its objects are: 1. failed(1) 2. passed(2)
atAtmfSummary	atmf 2	
atAtmfSummaryNodeName	atAtmfSummary 1	The name assigned to a particular node.
atAtmfSummaryStatus	atAtmfSummary 2	The Node's ATMF status.
atAtmfSummaryRole	atAtmfSummary 3	The role configured for this ATMF device, either Master or Member.
atAtmfSummaryNetworkName	atAtmfSummary 4	The ATMF network that a particular node belongs to.
atAtmfSummaryParentName	atAtmfSummary 5	The parent name of the node or 'none'.
atAtmfSummaryCoreDistance	atAtmfSummary 6	The ATMF core distance for this node.
atAtmfSummaryDomainId	atAtmfSummary 7	The ATMF domain Id for this node.
atAtmfSummaryRestrictedLogin	atAtmfSummary 8	The login for this ATMF device is restricted to only those devices that are designated ATMF Masters. Its objects are: 1. disabled(1) 2. enabled(2)
atAtmfSummaryNodes	atAtmfSummary 9	The number of ATMF nodes known to this device.
atAtmfNodeTable	atmf 3	ATMF Node Entry.
atAtmfNodeName	atAtmfNodeTable 1	The name assigned to a particular node.

AT-BOARDS-MIB

AT-BOARDS-MIB defines object identifiers for components of Allied Telesis products—base CPU and expansion boards, interface types, and chip sets. Objects in this MIB have the object identifier objects ({ atRouter 1 }), and are organized into the following groups:

- Base CPU and expansion boards (**Table 68-3**). These object identifiers are for use with the hrDeviceID object in the Host Resources MIB (see **"Public MIBs" on page 68.83**).
- Interface types (**Table 68-4**).
- Chip sets (**Table 68-5**).

Table 68-3: Object identifiers for base CPU and expansion boards

Object	Object Identifier	Description
boards	{ objects 1 }	
pprx90024XT	{ boards 271 }	x900-24XT Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays
pprx90024XS	{ boards 272 }	x900-24XS Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays
pprAtXum10Gi	{ boards 273 }	XEM-1XP Expansion Module, 1 x 10Gbe XFP port
pprAtXum12SFPi	{ boards 274 }	XEM-12S Expansion Module, 12 x SFP Gigabit ports
pprAtXum12Ti	{ boards 275 }	XEM-12T Expansion Module, 12 x 10/100/100BASE-T copper ports (RJ-45 connectors)
pprAtXum12TiN	{ boards 280 }	XEM-12T-N Expansion Module, 12 x 10/100/100BASE-T copper ports (RJ-45 connectors), NEBS compliant
pprx90024XTN	{ boards 281 }	x900-24XT Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays, NEBS compliant
pprSwitchBladex908	{ boards 282 }	Switchblade x908 8 Slot Layer 3 Switch Chassis
pprx90012XTS	{ boards 288 }	AT-x900-12XT/S Advanced Gigabit Layer 3+ Expandable Switch, 12 x combo ports (10/100/1000BASE-T copper or SFP), 1 x 30Gbps expansion bay
pprAt9524TS	{ boards 290 }	x600-24Ts/XP, 24 x 1000BASE-T ports (RJ45 connectors), 4 x SFP (combo) ports
pprAt9524TSXP	{ boards 291 }	x600-24Ts/XP, 24 x 1000BASE-T ports (RJ45 connectors), 4 x SFP (combo) ports, 2 x XFP ports
pprAt9548TS	{ boards 294 }	x600-44Ts, 44 x 1000BASE-T ports, 4 x SFP ports
pprAt9548TSXP	{ boards 295 }	x600-44Ts/XP, 44 x 1000BASE-T ports, 4 x SFP ports, 2 x XFP ports
pprXem2XP	{ boards 306 }	XEM-2XP Expansion Module, 2 x 10Gbe XFP port
pprATStackXG	{ boards 307 }	x600 Expansion Module, Stacking
pprATEMXP	{ boards 308 }	x600 Expansion Module, 2 x 10G XFP ports
pprATLBM	{ boards 309 }	x600 Expansion Module, loopback
pprAtSBx8112	{ boards 316 }	AT-SBx8112, SwitchBlade x8112 chassis
pprAtSBx81CFC400	{ boards 317 }	AT-SBx81CFC, Control Fabric Card for SwitchBlade x8112
pprAtSBx81GP24	{ boards 318 }	AT-SBx81GP24, 24 x 1G PoE line card
pprAtSBxPWRSYSAC	{ boards 320 }	AT-SBxPWR SYS/AC, system power supply unit for the SwitchBlade x8112 (AC input)

Table 68-3: Object identifiers for base CPU and expansion boards(cont.)

Object	Object Identifier	Description
pprAtSBxPWRPOEAC	{ boards 321 }	AT-SBxPWR POE/AC, PoE power supply unit for the SwitchBlade x8112 (AC input)
pprAtSBxFAN12	{ boards 322 }	AT-SBxFAN12, fan tray for the SwitchBlade x8112
pprAtPWR05DC	{ boards 323 }	AT-PWR05, DC power supply unit for SwitchBlade x908
pprXem2XT	{ boards 325 }	XEM-2XT Expansion Module, 2 x 10Gbe copper XEM port
pprx60024TSPOE	{ boards 326 }	x600-24Ts-POE, 24 x 1000BASE-T PoE ports (RJ45 connectors), 4 x SFP (combo) ports
pprx60024TSPOEPLUS	{ boards 327 }	x600-24Ts-POE+, 24 x 1000BASE-T PoE+ ports (RJ45 connectors), 4 x SFP (combo) ports
pprx61048TsXPOEPlus	{ boards 331 }	x610-48Ts/X-POE+, 48 x 1000BASE-T PoE+ ports (RJ45 connectors), 2 x SFP (combo) ports, 2 x SFP+ ports
pprx61048TsPOEPlus	{ boards 332 }	x610-48Ts-POE+, 48 x 1000BASE-T PoE+ ports (RJ45 connectors), 4 x SFP (combo) ports
pprx61024TsXPOEPlus	{ boards 333 }	x610-24Ts/X-POE+, 24 x 1000BASE-T PoE+ ports (RJ45 connectors), 4 x SFP (combo) ports, 2 x SFP+ ports
pprx61024TsPOEPlus	{ boards 334 }	x610-24Ts-POE+, 24 x 1000BASE-T PoE+ ports (RJ45 connectors), 4 x SFP (combo) ports
pprPWR800	{ boards 336 }	AT-PWR800, 800W power supply unit
pprPWR1200	{ boards 337 }	AT-PWR1200, 1200W power supply unit
pprPWR250	{ boards 338 }	AT-PWR250, 250W power supply unit
pprx61048TsX	{ boards 339 }	x610-48Ts/X, 48 x 1000BASE-T ports (RJ45 connectors), 2 x SFP (combo) ports, 2 x SFP+ ports
pprx61048Ts	{ boards 340 }	x610-48Ts, 48 x 1000BASE-T ports (RJ45 connectors), 4 x SFP (combo) ports
pprx61024TsX	{ boards 341 }	x610-24Ts/X, 24 x 1000BASE-T ports (RJ45 connectors), 4 x SFP (combo) ports, 2 x SFP+ ports
pprx61024Ts	{ boards 342 }	x610-24Ts, 24 x 1000BASE-T ports (RJ45 connectors), 4 x SFP (combo) ports
pprPWR250DC	{ boards 351 }	AT-PWR250DC, 250W DC power supply unit
pprAtSBx81GT24	{ boards 352 }	AT-SBx81GT24, 24 x 1G copper line card
pprAtSBx81GS24a	{ boards 353 }	AT-SBx81GS24a, 24 x 1G SFP line card
pprAtSBx81XS6	{ boards 354 }	AT-SBx81XS6, 6 x 10G SFP+ line card
pprx2109GT	{ boards 367 }	AT-x210-9GT, 8xGigbit, 1xSFP/T
pprx21016GT	{ boards 368 }	AT-x210-16GT, 14xGigbit, 2xcombo SFP/T
pprx21024GT	{ boards 369 }	AT-x210-24GT, 20xGigbit, 4xcombo SFP/T
pprx51028GTX	{ boards 370 }	AT-x510-28GTX board with 24 10/100/1000 Base-T ports and four 10Gb/s SFP+ ports.
pprx51028GPX	{ boards 371 }	AT-x510-28GPX board with 24 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports and PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
pprx51028GSX	{ boards 372 }	AT-x510-28GSX with 24 100/1000 SFP ports and four 10 Gb/s SFP+ ports.
pprx51052GTX	{ boards 373 }	AT-x510-52GTX board with 48 10/100/1000 Base-T ports and four 10 Gb/s SFP+ ports.
pprx51052GPX	{ boards 374 }	AT-x510-52GPX board with 48 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports and PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.

Table 68-3: Object identifiers for base CPU and expansion boards(cont.)

Object	Object Identifier	Description
pprAtSBx8106	{ boards 375 }	AT-SBx8106, SwitchBlade x8106 chassis
pprAtSBxFAN06	{ boards 376 }	AT-SBxFAN06, fan tray for the SwitchBlade x8106
pprAtSBx81CFC960	{ boards 377 }	AT-SBx81CFC960 Control Fabric Card for SwitchBlade x8100 Series chassis, four 10GbE SFP+ ports.
pprAtSBx81GT40	{ boards 381 }	AT-SBx81GT40 RJ point five line card.
pprPWR100R	{ boards 384 }	AT-PWR100R, 100W power supply unit
pprPWR250DCR	{ boards 385 }	AT-PWR250R-DC, 250W DC power supply unit
pprx510DP52GTX	{ boards 386 }	AT-x510DP-52GTX board with 48 10/100/1000 Base-T ports and four 10 Gb/s SFP+ ports.
pprxIX528GPX	{ boards 387 }	AT-IX5-28GPX board with 24 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports and PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
pprx31026FT	{ boards 393 }	AT-x310-26FT board with 24 10/100 Base-T ports, two 10/100/1000 Base-T ports, and four 10 Gb/s SFP+ ports.
pprx31050FT	{ boards 394 }	AT-x310-50FT board with 48 10/100 Base-T ports, two 10/100/1000 Base-T ports, and four 10 Gb/s SFP+ ports.
pprx31026FP	{ boards 395 }	AT-x310-26FP board with 24 10/100 Base-T ports, two 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports, plus PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
pprx31050FP	{ boards 396 }	AT-x310-50FP board with 48 10/100 Base-T ports, two 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports, plus PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
pprIE2006GT	{ boards 410 }	IE200-6GT L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports and 2 x SFP uplinks (100/1000X). Note that this is a single board device.
pprIE2006GP	{ boards 411 }	IE200-6GP L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports (with 802.3at PoE+) and 2 x SFP uplinks (100/1000X). Note that this is a single board device.
pprIE2006GPW	{ boards 412 }	IE200-6GPW L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports (with 802.3at PoE+) and 2 x SFP uplinks (100/1000X) and 802.11bgn wireless. Note that this is a single board device.

Table 68-4: Object identifiers for interface types

Object	Object Identifier	Description
iftypes	{ objects 3 }	
ifaceEth	{ iftypes 1 }	Ethernet
ifaceSyn	{ iftypes 2 }	Synchronous
ifaceAsyn	{ iftypes 3 }	Asynchronous
ifaceBri	{ iftypes 4 }	BRI ISDN
ifacePri	{ iftypes 5 }	PRI ISDN
ifacePots	{ iftypes 6 }	POTS (voice)
ifaceGBIC	{ iftypes 7 }	GBIC (Gigabit Interface Converter)
chipMips_4kcCpu	{ chips 6 }	Dual MIPS CPU

Table 68-5: Object identifiers for chip sets

Object	Object Identifier	Description
chips	{ objects 4 }	
chip68020Cpu	{ chips 1 }	MC68020 CPU
chip68340Cpu	{ chips 2 }	MC68340 CPU
chip68302Cpu	{ chips 3 }	MC68302 CPU
chip68360Cpu	{ chips 4 }	MC68360 CPU
chip860TCpu	{ chips 5 }	MPC860T CPU
chipMips4kcCpu	{ chips 6 }	Dual MIPS CPU
chipRtc1	{ chips 21 }	Real Time Clock v1
chipRtc2	{ chips 22 }	Real Time Clock v2
chipRtc3	{ chips 23 }	Real Time Clock v3
chipRtc4	{ chips 24 }	Real Time Clock v4
chipRam1mb	{ chips 31 }	1 MB RAM
chipRam2mb	{ chips 32 }	2 MB RAM
chipRam3mb	{ chips 33 }	3 MB RAM
chipRam4mb	{ chips 34 }	4 MB RAM
chipRam6mb	{ chips 36 }	6 MB RAM
chipRam8mb	{ chips 38 }	8 MB RAM
chipRam12mb	{ chips 42 }	12 MB RAM
chipRam16mb	{ chips 46 }	16 MB RAM
chipRam20mb	{ chips 50 }	20 MB RAM
chipRam32mb	{ chips 62 }	32 MB RAM
chipFlash1mb	{ chips 71 }	1 MB FLASH memory
chipFlash2mb	{ chips 72 }	2 MB FLASH memory
chipFlash3mb	{ chips 73 }	3 MB FLASH memory
chipFlash4mb	{ chips 74 }	4 MB FLASH memory
chipFlash6mb	{ chips 76 }	6 MB FLASH memory
chipFlash8mb	{ chips 78 }	8 MB FLASH memory
chipPem	{ chips 120 }	Processor Enhancement Module

AT-DHCPSN-MIB

This MIB contains objects for displaying and managing DHCP snooping and ARP security information on the switch. (**Table 68-6**). The objects reside in the module atDhcpsn { modules 537 }, organized in the following groups:

- The DHCP Snooping Events group (atDhcpsnEvents) contains notifications (traps)
- The DHCP Snooping table (atDhcpsnVariablesTable) contains DHCP snooping information
- The ARP Security table (atArpsecVariablesTable) contains ARP security information

Table 68-6: Objects defined in AT-DHCPSN-MIB

Object	Object Identifier	Description
atDhcpsn	{ modules 537 }	This MIB file contains definitions of managed objects for DHCP Snooping in AlliedWare Plus™.
atDhcpsnEvents	{ atDhcpsn 1 }	DHCP Snooping notifications (traps)
atDhcpsnTrap	{ atDhcpsnEvents 1 }	DHCP Snooping violation notification.
atArpsecTrap	{ atDhcpsnEvents 2 }	DHCP Snooping ARP Security violation notification.
atDhcpsnVariablesTable	{ atDhcpsn 1 }	The DHCP Snooping table. This table contains rows of DHCP Snooping information.
atDhcpsnVariablesEntry	{ atDhcpsnVariablesTable 1 }	A set of parameters that describe the DHCP Snooping features.
atDhcpsnIfIndex	{ atDhcpsnVariablesEntry 1 }	Ifindex of the port that the packet was received on.
atDhcpsnVid	{ atDhcpsnVariablesEntry 2 }	VLAN ID of the port that the packet was received on.
atDhcpsnSmac	{ atDhcpsnVariablesEntry 3 }	Source MAC address of the packet that caused the trap.
atDhcpsnOpcode	{ atDhcpsnVariablesEntry 4 }	Opcode value of the BOOTP packet that caused the trap. Only bootpRequest(1) or bootpReply(2) is valid.
atDhcpsnCiaddr	{ atDhcpsnVariablesEntry 5 }	Ciaddr value of the BOOTP packet that caused the trap.
atDhcpsnYiaddr	{ atDhcpsnVariablesEntry 6 }	Yiaddr value of the BOOTP packet that caused the trap.
atDhcpsnGiaddr	{ atDhcpsnVariablesEntry 7 }	Giaddr value of the BOOTP packet that caused the trap.
atDhcpsnSiaddr	{ atDhcpsnVariablesEntry 8 }	Siaddr value of the BOOTP packet that caused the trap.
atDhcpsnChaddr	{ atDhcpsnVariablesEntry 9 }	Chaddr value of the BOOTP packet that caused the trap.

Table 68-6: Objects defined in AT-DHCPSN-MIB(cont.)

Object	Object Identifier	Description
atDhcpsnVioType	{ atDhcpsnVariablesEntry 10 }	The reason that the trap was generated. ■ invalidBootp(1) indicates that the received BOOTP packet was invalid. For example, it is neither BootpRequest nor BootpReply. ■ invalidDhcpAck(2) indicates that the received DHCP ACK was invalid. ■ invalidDhcpRelDec(3) indicates the DHCP Release or Decline was invalid. ■ invalidIp(4) indicates that the received IP packet was invalid. ■ maxBindExceeded(5) indicates that if the entry was added, the maximum bindings configured for the port would be exceeded. ■ opt82InsertErr(6) indicates that the insertion of Option 82 failed. ■ opt82RxInvalid(7) indicates that the received Option 82 information was invalid. ■ opt82RxUntrusted(8) indicates that Option 82 information was received on an untrusted port. ■ opt82TxUntrusted(9) indicates that Option 82 would have been transmitted out an untrusted port. ■ replyRxUntrusted(10) indicates that a BOOTP Reply was received on an untrusted port. ■ srcMacChaddrMismatch(11) indicates that the source MAC address of the packet did not match the BOOTP CHADDR of the packet. ■ staticEntryExisted(12) indicates that the static entry to be added already exists. ■ dbAddErr(13) indicates that adding an entry to the database failed.
atArpsecVariablesTable	{ atDhcpsn 2 }	The ARP Security table. This table contains rows of DHCP Snooping ARP Security information.
atArpsecVariablesEntry	{ atArpsecVariablesTable 1 }	A set of parameters that describe the DHCP Snooping ARP Security features.
atArpsecIfIndex	{ atArpsecVariablesEntry 1 }	Ifindex of the port that the ARP packet was received on.
atArpsecClientIP	{ atArpsecVariablesEntry 2 }	Source IP address of the ARP packet.
atArpsecSrcMac	{ atArpsecVariablesEntry 3 }	Source MAC address of the ARP packet.
atArpsecVid	{ atArpsecVariablesEntry 4 }	VLAN ID of the port that the ARP packet was received on.

Table 68-6: Objects defined in AT-DHCPSN-MIB(cont.)

Object	Object Identifier	Description
atArpsecVioType	{ atArpsecVariablesEntry 5 }	The reason that the trap was generated. ■ srcIpNotFound(1) indicates that the Sender IP address of the ARP packet was not found in the DHCP Snooping database. ■ badVLAN(2) indicates that the VLAN of the DHCP Snooping binding entry associated with the Sender IP address of the ARP packet does not match the VLAN that the ARP packet was received on. ■ badPort(3) indicates that the port of the DHCP Snooping binding entry associated with the Sender IP address of the ARP packet does not match the port that the ARP packet was received on. ■ srcIpNotAllocated(4) indicates that the CHADDR of the DHCP Snooping binding entry associated with the Sender IP address of the ARP packet does not match the Source MAC and/or the ARP source MAC of the ARP packet.

AT-DNS-CLIENT-MIB

AT-DNS-CLIENT-MIB contains definitions of managed objects for the Allied Telesis DNS Client Configuration.

Objects in this group have the object identifier atDns ({ Modules 501 }). **Table 68-7** lists the objects supported by the AlliedWare Plus™ Operating System.

Table 68-7: Objects defined in AT-DNS-CLIENT-MIB

Object	Object Identifier	Description
atDnsClient	{ atDns 1 }	MIB File for DNS Client Configuration.
atDNSServerIndexNext	{ atDnsClient 1 }	The next available value for the object 'atDNSServerIndex'. The value is used by a management application to create an entry in the 'atDNSServerTable'.
atDNSServerTable	{ atDnsClient 2 }	Table of information about the Domain Name System (DNS) Server configurations in the system, indexed by 'atDNSServerIndex'.
atDNSServerEntry	{ atDNSServerTable 1 }	Information about a single DNS Server Configuration.
atDNSServerIndex	{ atDNSServerEntry 1 }	The index corresponding to the particular DNS Server Configuration. When creating a new entry in the table, the value of this object must be equal to the value in the 'atDNSServerIndexNext'.
atDNSServerAddrType	{ atDNSServerEntry 2 }	The Internet Address Type of the 'atDNSServerAddr' object. Can be one of the following: unknown (0) 1. ipv4 (1) - default 2. ipv6 (2) - not supported 3. ipv4z (3) - not supported 4. ipv6z (4) - not supported 5. dns (16) - not supported
atDNSServerAddr	{ atDNSServerEntry 3 }	The IP Address of the DNS Server. When a new entry is created, this object is set to the default of '0.0.0.0' { '00000000'h }. The management application will change this to the desired value using a SET operation.
atDNSServerStatus	{ atDNSServerEntry 4 }	The status of the current entry (row). Can be one of the following: 1. active (1) 2. createAndGo (4) 3. destroy (6) To create a new entry the management application must set this object with value 'createAndGo (4)'. To delete an entry, the management application must set this object with value 'destroy (6)'. Once an entry is deleted, all subsequent entries in the table will be renumbered. The default is 1 (active)

AT-ENVMONv2-MIB

The AT Environment Monitoring v2 MIB (atEnvMonv2-MIB) has the object path 207.8.4.4.3.12. It contains objects for managing and reporting data relating to fans, voltage rails, temperature sensors and power supply units installed in the device (**Table 68-8**). Objects in this group have the object identifier EnvMonv2 ({ sysinfo 12 }).

Table 68-8: Objects defined in AT-ENVMONV2-MIB

Object / Object Identifier	Description
atEnvMonv2Notifications { atEnvMonv2 0 } OID (207.8.4.4.3.12.0)	A collection of traps (notification) objects for monitoring fans, voltage rails, temperature sensors, and power supply bays.
atEnvMonv2FanAlarmSetNotify { atEnvMonv2Notifications 1 } OID (207.8.4.4.3.12.0.1)	A notification that is generated when the monitored speed of a fan drops below its lower threshold. It returns the value of: 1. atEnvMonv2FanStackMemberId 2. atEnvMonv2FanBoardIndex 3. atEnvMonv2FanIndex 4. atEnvMonv2FanDescription 5. atEnvMonv2FanLowerThreshold 6. atEnvMonv2FanCurrentSpeed
atEnvMonv2FanAlarmClearedNotify { atEnvMonv2Notifications 2 }	Notification generated when the monitored speed of a fan returns to an acceptable value, the fan having previously been in an alarm condition. It returns the value of: 1. atEnvMonv2FanStackMemberId 2. atEnvMonv2FanBoardIndex 3. atEnvMonv2FanIndex 4. atEnvMonv2FanDescription 5. atEnvMonv2FanLowerThreshold 6. atEnvMonv2FanCurrentSpeed
atEnvMonv2VoltAlarmSetNotify { atEnvMonv2Notifications 3 }	Notification generated when the voltage of a monitored voltage rail, goes out of tolerance by either dropping below its lower threshold, or exceeding its upper threshold. It returns the value of: 1. atEnvMonv2VoltageStackMemberId 2. atEnvMonv2VoltageBoardIndex 3. atEnvMonv2VoltageIndex 4. atEnvMonv2VoltageDescription 5. atEnvMonv2VoltageUpperThreshold 6. atEnvMonv2VoltageLowerThreshold 7. atEnvMonv2VoltageCurrent (i.e. the voltage currently being measured).
atEnvMonv2VoltAlarmClearedNotify { atEnvMonv2Notifications 4 }	Notification generated when the voltage of a monitored voltage rail returns to an acceptable value, having previously been in an alarm condition. It returns the value of: 1. atEnvMonv2VoltageStackMemberId 2. atEnvMonv2VoltageBoardIndex 3. atEnvMonv2VoltageIndex 4. atEnvMonv2VoltageDescription 5. atEnvMonv2VoltageUpperThreshold 6. atEnvMonv2VoltageLowerThreshold 7. atEnvMonv2VoltageCurrent (i.e. the voltage currently being measured).

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2TempAlarmSetNotify { atEnvMonv2Notifications 5 }	Notification generated when a monitored temperature exceeds its upper threshold. It returns the value of: 1. atEnvMonv2TemperatureStackMemberId 2. atEnvMonv2TemperatureBoardIndex 3. atEnvMonv2TemperatureIndex 4. atEnvMonv2TemperatureDescription 5. atEnvMonv2TemperatureUpperThreshold 6. atEnvMonv2TemperatureCurrent
atEnvMonv2TempAlarmClearedNotify { atEnvMonv2Notifications 6 }	Notification generated when a monitored temperature returns to an acceptable value, having previously been in an alarm condition. It returns the value of: 1. atEnvMonv2TemperatureStackMemberId 2. atEnvMonv2TemperatureBoardIndex 3. atEnvMonv2TemperatureIndex 4. atEnvMonv2TemperatureDescription 5. atEnvMonv2TemperatureUpperThreshold
atEnvMonv2PsbAlarmSetNotify { atEnvMonv2Notifications 7 }	Notification generated when a monitored parameter of a power supply bay device goes out of tolerance. It returns the value of: 1. atEnvMonv2PsbSensorStackMemberId 2. atEnvMonv2PsbSensorBoardIndex 3. atEnvMonv2PsbSensorIndex 4. atEnvMonv2PsbSensorType 5. atEnvMonv2PsbSensorDescription
atEnvMonv2PsbAlarmClearedNotify { atEnvMonv2Notifications 8 }	Notification generated when a monitored parameter of a power supply bay device returns to an acceptable value, having previously been in an alarm condition. It returns the value of: 1. atEnvMonv2PsbSensorStackMemberId 2. atEnvMonv2PsbSensorBoardIndex 3. atEnvMonv2PsbSensorIndex 4. atEnvMonv2PsbSensorType 5. atEnvMonv2PsbSensorDescription
atEnvMonv2ContactInputOpenNotify { atEnvMonv2Notifications 9 }	Notification generated when a monitored contact input opens. It returns the value of: 1. atEnvMonv2ContactInputStackMemberId 2. atEnvMonv2ContactInputBoardIndex 3. atEnvMonv2ContactInputIndex 4. atEnvMonv2ContactInputDescription
atEnvMonv2ContactInputCloseNotify { atEnvMonv2Notifications 10 }	Notification generated when a monitored contact input closes. It returns the value of: 1. atEnvMonv2ContactInputStackMemberId 2. atEnvMonv2ContactInputBoardIndex 3. atEnvMonv2ContactInputIndex 4. atEnvMonv2ContactInputDescription

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2ExternalPSUAlarmSetNotify { atEnvMonv2Notifications 11 }	Notification generated when supply potential of a monitored external power supply is not present. It returns the value of: 1. atEnvMonv2ExternalPSUStackMemberId 2. atEnvMonv2ExternalPSUBoardIndex 3. atEnvMonv2ExternalPSUIndex 4. atEnvMonv2ExternalPSUDescription
atEnvMonv2ExternalPSUAlarmClearedNotify { atEnvMonv2Notifications 12 }	Notification generated when supply potential of a monitored external power supply returns to an acceptable level, having previously been in alarm condition. It returns the value of: 1. atEnvMonv2ExternalPSUStatusStackMemberId 2. atEnvMonv2ExternalPSUStatusBoardIndex 3. atEnvMonv2ExternalPSUStatusIndex 4. atEnvMonv2ExternalPSUStatusDescription
atEnvMonv2FanTable { EnvMonv2 1 } OID (207.8.4.4.3.12.1)	Table of information about fans installed in the device that have their fan speeds monitored by environment monitoring hardware, indexed by: 1. atEnvMonv2FanStackMemberId 2. atEnvMonv2FanBoardIndex 3. atEnvMonv2FanIndex
atEnvMonv2FanEntry { atEnvMonv2FanTable 1 }	Description, current speed, lower threshold speed and current status of a single fan.
atEnvMonv2FanStackMemberId { atEnvMonv2FanEntry 1 }	Index of the stack member hosting this fan.
atEnvMonv2FanBoardIndex { atEnvMonv2FanEntry 2 }	Index of the board hosting this fan in the board table.
atEnvMonv2FanIndex { atEnvMonv2FanEntry 3 }	Numeric identifier of this fan on its host board.
atEnvMonv2FanDescription { atEnvMonv2FanEntry 4 }	Description of this fan.
atEnvMonv2FanCurrentSpeed { atEnvMonv2FanEntry 5 }	Current speed of this fan in revolutions per minute.
atEnvMonv2FanLowerThreshold { atEnvMonv2FanEntry 6 }	Minimum acceptable speed of the fan in revolutions per minute.
atEnvMonv2FanStatus { atEnvMonv2FanEntry 7 }	Whether this fan is currently in an alarm condition. The values can be: 1. Failed. Means that the current speed is too low. 2. Good. Means that the current speed is acceptable.
atEnvMonv2VoltageTable { atEnvMonv2 2 }	Table of information about voltage rails in the device that are monitored by environment monitoring hardware, indexed by: 1. atEnvMonv2VoltageStackMemberId ■ atEnvMonv2VoltageBoardIndex ■ atEnvMonv2VoltageIndex
atEnvMonv2VoltageEntry { atEnvMonv2VoltageTable 1 }	Description, current value, upper & lower threshold settings and current status of a single voltage rail.
atEnvMonv2VoltageStackMemberId { atEnvMonv2VoltageEntry 1 }	Index of the stack member hosting this voltage sensor.

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2VoltageBoardIndex { atEnvMonv2VoltageEntry 2 }	Index of the board hosting this voltage sensor in the board table.
atEnvMonv2VoltageIndex { atEnvMonv2VoltageEntry 3 }	Numeric identifier of this voltage rail on its host board.
atEnvMonv2VoltageDescription { atEnvMonv2VoltageEntry 4 }	Description of this voltage rail.
atEnvMonv2VoltageCurrent { atEnvMonv2VoltageEntry 5 }	Current reading of this voltage rail in millivolts.
atEnvMonv2VoltageUpperThreshold { atEnvMonv2VoltageEntry 6 }	Maximum acceptable reading of this voltage rail in millivolts.
atEnvMonv2VoltageLowerThreshold { atEnvMonv2VoltageEntry 7 }	Minimum acceptable reading of this voltage rail in millivolts.
atEnvMonv2VoltageStatus { atEnvMonv2VoltageEntry 8 }	Whether this voltage rail is currently in an alarm condition. Possible values are: 1. outOfRange (1) - means that the current reading is outside the threshold range. 2. inRange (2) - means that the current reading is acceptable.
atEnvMonv2TemperatureTable { atEnvMonv2 3 }	Table of information about temperature sensors in the device that are monitored by environment monitoring hardware, indexed by: 1. atEnvMonv2TemperatureStackMemberId 2. atEnvMonv2TemperatureBoardIndex 3. atEnvMonv2TemperatureIndex 4. atEnvMonv2TemperatureDescription 5. atEnvMonv2TemperatureCurrent 6. atEnvMonv2TemperatureUpperThreshold 7. atEnvMonv2TemperatureStatus
atEnvMonv2TemperatureEntry { atEnvMonv2TemperatureTable 1 }	Description, current value, upper threshold setting and current status of a single temperature sensor.
atEnvMonv2TemperatureStackMemberId { atEnvMonv2TemperatureEntry 1 }	Index of the stack member hosting this temperature sensor.
atEnvMonv2TemperatureBoardIndex { atEnvMonv2TemperatureEntry 2 }	Index of the board hosting this temperature sensor in the board table.
atEnvMonv2TemperatureIndex { atEnvMonv2TemperatureEntry 3 }	Numeric identifier of this temperature sensor on its host board.
atEnvMonv2TemperatureDescription { atEnvMonv2TemperatureEntry 4 }	Description of this temperature sensor.
atEnvMonv2TemperatureCurrent { atEnvMonv2TemperatureEntry 5 }	Current reading of this temperature sensor in degrees Celsius.
atEnvMonv2TemperatureUpperThreshold { atEnvMonv2TemperatureEntry 6 }	Maximum acceptable reading for this temperature sensor in degrees Celsius.
atEnvMonv2TemperatureStatus { atEnvMonv2TemperatureEntry 7 }	Whether this temperature sensor is currently in an alarm condition. Can be: 1. outOfRange (1) - means that the current reading is outside the threshold range. 2. inRange (2) - means that the current reading is acceptable.

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2PsbObjects { atEnvMonv2 4 }	Collection of objects for monitoring power supply bays in the system and any devices that are installed. It contains the following objects: 1. atEnvMonv2PsbTable ■ atEnvMonv2PsbSensorTable
atEnvMonv2PsbTable { atEnvMonv2PsbObjects 1 }	Table of information about power supply bays in the system, indexed by: 1. atEnvMonv2PsbHostStackMemberId 2. atEnvMonv2PsbHostBoardIndex 3. atEnvMonv2PsbHostSlotIndex 4. atEnvMonv2PsbHeldBoardIndex 5. atEnvMonv2PsbHeldBoardId 6. atEnvMonv2PsbDescription
atEnvMonv2PsbEntry { atEnvMonv2PsbTable 1 }	Description and current status of a single power supply bay device.
atEnvMonv2PsbHostStackMemberId { atEnvMonv2PsbEntry 1 }	Index of the stack member hosting this power supply bay.
atEnvMonv2PsbHostBoardIndex { atEnvMonv2PsbEntry 2 }	Index of the board hosting this power supply bay in the board table.
atEnvMonv2PsbHostSlotIndex { atEnvMonv2PsbEntry 3 }	Index of this power supply bay slot on its host board. This index is fixed for each slot, on each type of board.
atEnvMonv2PsbHeldBoardIndex { atEnvMonv2PsbEntry 4 }	Index of a board installed in this power supply bay. This value corresponds to atEnvMonv2PsbSensorBoardIndex for each sensor on this board. A value of 0 indicates that a board is either not present or not supported.
atEnvMonv2PsbHeldBoardId { atEnvMonv2PsbEntry 5 }	Type of board installed in this power supply bay. The values of this object are taken from the pprXxx object IDs under the boards sub-tree in the parent MIB. A value of 0 indicates that a board is either not present or not supported.
atEnvMonv2PsbDescription { atEnvMonv2PsbEntry 6 }	Description of this power supply bay.
atEnvMonv2PsbSensorTable { atEnvMonv2PsbObjects 2 }	Table of information about environment monitoring sensors on devices installed in power supply bays, indexed by: 1. atEnvMonv2PsbSensorStackMemberId ■ atEnvMonv2PsbSensorBoardIndex ■ atEnvMonv2PsbSensorIndex
atEnvMonv2PsbSensorEntry { atEnvMonv2PsbSensorTable 1 }	Description and current status of the sensor on a device installed in a power supply bay.
atEnvMonv2PsbSensorStackMemberId { atEnvMonv2PsbSensorEntry 1 }	Index of the stack member hosting this sensor.
atEnvMonv2PsbSensorBoardIndex { atEnvMonv2PsbSensorEntry 2 }	Index of the board hosting this sensor in the board table.
atEnvMonv2PsbSensorIndex { atEnvMonv2PsbSensorEntry 3 }	Index of this power supply bay environmental sensor on its host board.

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2PsbSensorType { atEnvMonv2PsbSensorEntry 4 }	Type of environmental variable this sensor detects. One of: 1. psbSensorTypeInvalid(0) ■ fanSpeedDiscrete(1) ■ temperatureDiscrete(2) ■ voltageDiscrete(3)
atEnvMonv2PsbSensorDescription { atEnvMonv2PsbSensorEntry 5 }	Description of this power supply bay environmental sensor.
atEnvMonv2PsbSensorStatus { atEnvMonv2PsbSensorEntry 6 }	Whether this environmental sensor is currently in an alarm condition. One of: 1. failed (1) - the device is in a failure condition 2. good (2) - the device is functioning normally. 3. notPowered (3) - a PSU is installed, but not powered up
atEnvMonv2PsbSensorReading { atEnvMonv2PsbSensorEntry 7 }	An indication of whether this environmental sensor is currently reading a value for the monitored device. A value of 'no' indicates that there is no current reading, 'yes' indicates that the monitored device is supplying a reading. 1. no 2. yes
atEnvMonv2Traps { atEnvMonv2 5 } (207.8.4.4.3.12.5)	Note that objects under this portion of the tree have been deprecated, and replaced by objects under the tree portion 207.8.4.4.3.12.0.
atEnvMonv2FaultLedTable { atEnvMonv2 6 }	Table detailing any LED fault indications on the device, indexed by: 1. atEnvMonv2FaultLedStackMemberId
atEnvMonv2FaultLedEntry { atEnvMonv2FaultLedTable 1 }	Information pertaining to a given fault LED.
atEnvMonv2FaultLedStackMemberId { atEnvMonv2FaultLedEntry 1 }	Index of the stack member hosting this fault LED.
atEnvMonv2FaultLed1Flash { atEnvMonv2FaultLedEntry 2 }	Indicates whether a fault LED is currently showing a system failure by flashing once. Values can be: 1. heatsinkFanFailure (1) - indicates that one or more heatsink fans have failed, or are operating below the recommended speed 2. noFault (2)
atEnvMonv2FaultLed2Flashes { atEnvMonv2FaultLedEntry 3 }	Indicates whether a fault LED is currently showing a system failure by flashing twice. Values can be: 1. chassisFanFailure (1) - indicates that one or both of the chassis fans are not installed, or the fans are operating below the recommended speed 2. noFault (2)
atEnvMonv2FaultLed3Flashes { atEnvMonv2FaultLedEntry 4 }	Indicates whether a fault LED is currently showing a system failure by flashing three times. Values can be: 1. sensorFailure (1) - indicates that the ability to monitor temperature or fans has failed 2. noFault (2)
atEnvMonv2FaultLed4Flashes { atEnvMonv2FaultLedEntry 5 }	Indicates whether a fault LED is currently showing a system failure by flashing four times. Values can be: 1. xemInitialisationFailure (1) - indicates that a XEM failed to initialise or is incompatible 2. noFault (2)

Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2FaultLed5Flashes { atEnvMonv2FaultLedEntry 6 }	Indicates whether a fault LED is currently showing a system failure by flashing five times. Values can be: 1. alarmMonitorAlarm (1) - indicates that the Alarm Monitor has detected one or more fault conditions. 2. noFault (2)
atEnvMonv2FaultLed6Flashes { atEnvMonv2FaultLedEntry 7 }	Indicates whether a fault LED is currently showing a system failure by flashing six times. Values can be: 1. temperatureFailure (1) - indicates that the device's temperature has exceeded the recommended threshold 2. noFault (2)
atEnvMonv2ContactInputTable { atEnvMonv2 7 } (1.3.6.1.4.1.207.8.4.4.3.12.7)	Table of information about contact inputs available in the device that are monitored by environment monitoring hardware, indexed by: ■ atEnvMonv2ContactInputStackMemberId ■ atEnvMonv2ContactInputBoardIndex ■ atEnvMonv2ContactInputIndex
atEnvMonv2ContactInputEntry { atEnvMonv2ContactInputTable 1 }	The description and current state of a contact input.
atEnvMonv2ContactInputStackMemberId { atEnvMonv2ContactInputEntry 1 }	Index of the stack member hosting this input contact.
atEnvMonv2ContactInputBoardIndex { atEnvMonv2ContactInputEntry 2 }	Index of the board hosting this input contact in the board table.
atEnvMonv2ContactInputIndex { atEnvMonv2ContactInputEntry 3 }	The numeric identifier of this contact input on its host board.
atEnvMonv2ContactInputDescription { atEnvMonv2ContactInputEntry 4 }	The description of this contact input.
atEnvMonv2ContactInputState { atEnvMonv2ContactInputEntry 5 }	Current state of the input contact - closed (1) or open (2).
atEnvMonv2ContactIOutputTable { atEnvMonv2 8}	Table of information about contact outputs available in the device that are managed by environment monitoring hardware, indexed by: 1. atEnvMonv2ContactOutputStackMemberId 2. atEnvMonv2ContactOutputBoardIndex 3. atEnvMonv2ContactOutputIndex
atEnvMonv2ContactOutputEntry { atEnvMonv2ContactOutputTable 1 }	
atEnvMonv2ContactOutputStackMemberId { atEnvMonv2ContactInputEntry 1 }	Index of the stack member hosting this output contact.
atEnvMonv2ContactOutputBoardIndex { atEnvMonv2ContactInputEntry 2 }	Index of the board hosting this contact output in the board table.
atEnvMonv2ContactOutputIndex { atEnvMonv2ContactInputEntry 3 }	The numeric identifier of this contact output on its host board.
atEnvMonv2ContactOutputDescription { atEnvMonv2ContactInputEntry 4 }	The description of this contact output.
atEnvMonv2ContactOutputState { atEnvMonv2ContactInputEntry 5 }	Current state of the output contact - closed (1) or open (2).

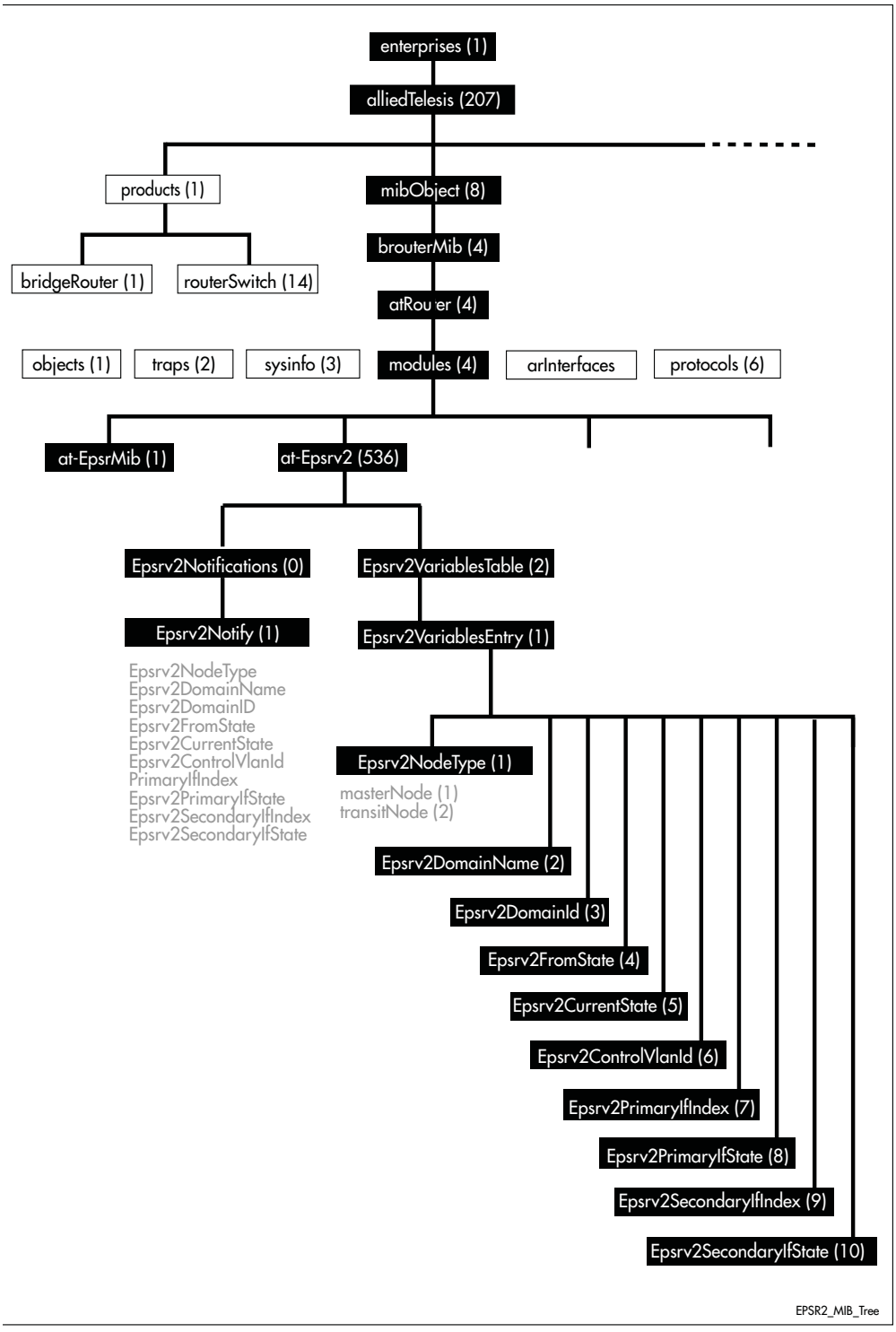
Table 68-8: Objects defined in AT-ENVMONV2-MIB(cont.)

Object / Object Identifier	Description
atEnvMonv2ExternalPSUTable { atEnvMonv2 9}	Table of information about external power supply status monitored by environment monitoring hardware, indexed by: 1. atEnvMonv2ExternalPSUStatusStackMemberId 2. atEnvMonv2ExternalPSUStatusBoardIndex 3. atEnvMonv2ExternalPSUStatusIndex
atEnvMonv2ExernalPSUEntry { atEnvMonv2ExternalPSUStatusTable 1 }	
atEnvMonv2ExternalPSUStackMemberId { atEnvMonv2ExternalPSUEntry 1 }	Index of the stack member hosting this external power supply.
atEnvMonv2ExternalPSUBoardIndex { atEnvMonv2ExternalPSUEntry 2 }	Index of the board hosting this external power supply in the board table.
atEnvMonv2ExternalPSUIndex { atEnvMonv2ExternalPSUEntry 3 }	The numeric identifier of this external power supply on its host board.
atEnvMonv2ExternalPSUDescription { atEnvMonv2ExternalPSUEntry 4 }	The description of this external power supply.
atEnvMonv2ExternalPSUState { atEnvMonv2ExternalPSUEntry 5 }	Current state of the output contact - good (1) or failed (2).

AT-EPSRv2-MIB

The EPSRv2 Group-MIB defines objects for managing Epsrv2 objects and triggers (**Figure 68-4**, **Table**). Objects in this group have the object identifier Epsrv2 ({ modules 536 }).

Figure 68-4: The AT-EPSRv2 MIB sub-tree



.

atEpsrv2Objects Defined in the AT-EPSRV2 MIB

Object	Object Identifier	Description
{ at-Epsrv2 }	{ modules 536 }	The root of the Epsrv2 object sub tree.
{ atEpsrv2Notifications }	{ at-Epsrv2 0 }	
{ atEpsrv2Notify }	{ atEpsrv2Notifications 1 }	EPSR Master/Transit node state transition trap. Note that there is a one to one relationship between nodes and domains.
{ Epsrv2NodeType }	{ atEpsrv2VariablesEntry 1 }	The EPSR node type: either master or transit.
{ atEpsrv2DomainName }	{ atEpsrv2VariablesEntry 2 }	The name of the EPSR domain.
{ atEpsrv2DomainID }	{ atEpsrv2VariablesEntry 3 }	The ID of the EPSR domain.
{ Epsrv2FromState }	{ atEpsrv2VariablesEntry 4 }	The previous state of the EPSR domain
{ Epsrv2Current State }	{ atEpsrv2VariablesEntry 5 }	The current state of the EPSR domain.
{ Epsrv2ControlVlanId }	{ atEpsrv2VariablesEntry 6 }	The VLAN identifier for the control VLAN.
{ Epsrv2PrimaryIfIndex }	{ atEpsrv2VariablesEntry 7 }	The IfIndex of the primary interface.
{ atEpsrv2PrimaryIfState }	{ atEpsrv2VariablesEntry 8 }	The current state of the primary interface.
{ atEpsrv2SecondaryIfIndex }	{ atEpsrv2VariablesEntry 9 }	The IfIndex of the secondary interface.
{ atEpsrv2SecondaryIfState }	{ atEpsrv2VariablesEntry 10 }	The state of the secondary interface.
{ atEpsrv2VariablesTable }	{ at-Epsrv2 2 }	The enterprise Epsrv2VariablesTable.
{ atEpsrv2VariablesEntry }	{ atEpsrv2VariablesTable 1}	Contains entries within the enterprise atEpsrv2VariablesTable.
{ atEpsrv2NodeType }	{ atEpsrv2VariablesEntry 1 }	The EPSR domain node type: either 1. master (1) 2. transit (2)
{ atEpsrv2DomainName }	{ Epsrv2NodeType 2 }	The name of the EPSR domain.
{ atEpsrv2DomainID }	{ Epsrv2NodeType 3 }	The ID of the EPSR domain.
{ atEpsrv2FromState }	{ Epsrv2NodeType 4 }	The previous state of the EPSR domain
{ atEpsrv2Current State }	{ Epsrv2NodeType 5 }	The current state of the EPSR domain.
{ atEpsrv2ControlVlanId }	{ Epsrv2NodeType 6 }	The VLAN identifier for the control VLAN.
{ Epsrv2PrimaryIfIndex }	{ Epsrv2NodeType 7 }	The IfIndex of the primary interface.
{ atEpsrv2PrimaryIfState }	{ Epsrv2NodeType 8 }	The current state of the primary interface.
{ atEpsrv2SecondaryIfIndex }	{ Epsrv2NodeType 9 }	The IfIndex of the secondary interface.
{ atEpsrv2SecondaryIfState }	{ Epsrv2NodeType 10 }	The state of the secondary interface.
TEXTUAL CONVENTIONS		
{ atEpsrv2NodeState }		The trap states that can be advertised for an EPSR domain node. The following states are defined: 1. idle (1) 2. complete (2) 3. failed (3) 4. linksUp (4) 5. linksDown (5) 6. preForward (6) 7. unknown (7)

atEpsrv2Objects Defined in the AT-EPSRV2 MIB(cont.)

Object	Object Identifier	Description
{ atEpsrv2InterfaceState }		The trap states that can be advertised for an EPSR interface. The following states are defined: 1. unknown (1) 2. down (2) 3. blocked (3) 4. forward (4)

AT-FILEv2-MIB

This MIB contains objects for displaying and managing file content of Flash, USB storage devices and NVS, and copying, moving and deleting files from local and remote sources (**Table 68-9**).

The objects reside in the module atFilev2 { modules 600 }, organized in the following groups:

- The file operation devices - object for various devices supported for file operations
- The File Info Table - information about all files, including pathnames, that are present on the device
- The USB storage device table - information about the USB storage device configured on the device

The procedure in **"Copy a File to or from a TFTP Server" on page 66.20** shows how to use these MIB objects to upgrade to a new software version and boot configuration file.

Table 68-9: Objects defined in AT-FILEv2-MIB

Object	Object Identifier	Description
atFilev2	{ modules 600 }	MIB containing objects for listing and managing files.
atFilev2FileOperation	{ atFilev2 3 }	Collection of file operation objects available for configuration, to enable copying, moving and deleting files.
atFilev2SourceStackID	{ atFilev2Operation 1 }	Specifies the Stack ID of the source file. Set an integer corresponding to the stack ID of the stack member to use as the source. For devices that are not capable of being stacked, set with the value 1. This value is ignored if the source device is set to TFTP.
atFilev2SourceDevice	{ atFilev2Operation 2 }	Specifies the source device for the file to be copied. Valid values are 1 to 5. Set a value that corresponds with the various devices, as below: ■ 1 - Flash - default ■ 2 - Card - not supported ■ 3 - NVS ■ 4 - TFTP ■ 5 - USB For copying files, you may use any combination of devices for the source and destination, except for copying from TFTP to TFTP. For moving files you cannot use TFTP as source or destination. For deleting files, the source cannot be TFTP. You must fully configure all required parameters before an operation can commence. Where a TFTP operation is configured, an IP address must also be set via atFilev2TftpIPAddr. To copy a file from TFTP to Flash, use 4 for source and 1 for destination.
atFilev2SourceFilename	{ atFilev2Operation 3 }	Specifies the filename of the source file to copy, move or delete. Include any path as required, but the storage type is not necessary. For example, to copy the file `latest.cfg` from the backupconfigs/routers directory on the TFTP server, you would set: `backupconfigs/routers/latest.cfg`

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2DestinationStackID	{ atFilev2Operation 4 }	Specifies the Stack ID for the destination file. For devices that are not capable of being stacked, set with the value 1. This value is ignored if the destination device is set to TFTP, or if a deletion operation is carried out.
atFilev2DestinationDevice	{ atFilev2Operation 5 }	Specifies the destination device for the files to be copied into. Valid values are 1 to 5. Set a value that corresponds with the various devices, as below: ■ 1 - Flash - default ■ 2 - Card - not supported ■ 3 - NVS ■ 4 - TFTP ■ 5 - USB For copying files, you may use any combination of devices for the source and destination, except for copying from TFTP to TFTP. For moving files you cannot use TFTP as source or destination. For deleting files, this object is ignored. You must fully configure all required parameters before an operation can commence. Where a TFTP operation is configured, an IP address must also be set via atFilev2TftpIPAddr. To copy a file from TFTP to Flash, use 4 for source and 1 for destination.
atFilev2DestinationFilename	{ atFilev2Operation 6 }	Specifies the destination filename of the file to be copied or moved. Include any path as required, but the storage type is not necessary. The destination filename does not need to be the same as the source filename, and this object is ignored for file deletion operations. For example, to copy a release file from the TFTP server to the backup release directory on Flash, you would set: `backuprelease/latest.rel` Note: If the destination is set to Flash, card or NVS, any file at the destination that shares the destination filename will be overwritten by a move or copy operation.

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2CopyBegin	{ atFilev2Operation 7 }	Represents the status of the copy file operation, in the form of octet string. A read on this object can return several possible values, depending on the current status of the system and the various file operation objects: ■ idle - There is no file operation in progress and all required objects have been set correctly. Setting a '1' to this object will begin the file copy. ■ Error codes: [1-7] - A copy operation cannot be started until these errors are resolved. See below for key. ■ [action]ing x [--> y] - A file operation is currently in progress. You cannot start another operation while the object is returning this value. ■ [action] x [--> y] success - The last copy, move or delete operation was successfully completed. ■ [action] x [--> y] failure: [err] - The last copy, move or delete operation failed, with the error message attached. Common failures include lack of space on the destination file system, incorrect source file names or communication errors with remote services. Upon reading a success or failure message, the message will be cleared and the next read will result in either an 'idle' message or an 'Error codes' message if not all required objects have been correctly set. If the read returned 'idle', a new file operation can now be started. Following are possible values returned as Error codes for file copy: ■ 1 - atFilev2SourceDevice has not been set ■ 2 - atFilev2SourceFilename has not been set ■ 3 - atFilev2DestinationDevice has not been set ■ 4 - atFilev2DestinationFilename has not been set ■ 5 - atFilev2SourceDevice and atFilev2DestinationDevice are both set to TFTP ■ 6 - the combination of source device, stackID and filename is the same as the destination device, stackID and filename (i.e. it is not valid to copy a file onto itself. ■ 7 - TFTP IP address has not been set and TFTP has been set for one of the devices Provided all above requirements are met, immediately upon executing the SNMP set, the device will indicate that it was a success. The actual file copy itself will be started and continue on the device until it has completed. For large files, operations can take several minutes to complete. Subsequent reads of the object will return one of messages shown in the first table, to allow for tracking of the progress of the copy operation.

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2MoveBegin	{ atFilev2Operation 8 }	Represents the status of the move file operation, in the form of octet string. A read on this object can return several possible values, depending on the current status of the system and the various file operation objects: ■ idle - There is no file operation in progress and all required objects have been set correctly. Setting a '1' to this object will begin the file move. ■ Error codes: [1-6] - A move operation cannot be started until these errors are resolved. See below for key. ■ [action]ing x [--> y] - A file operation is currently in progress. You cannot start another operation while the object is returning this value. ■ [action] x [--> y] success - The last copy, move or delete operation was successfully completed. ■ [action] x [--> y] failure: [err] - The last copy, move or delete operation failed, with the error message attached. Common failures include lack of space on the destination file system, incorrect source file names or communication errors with remote services. Upon reading a success or failure message, the message will be cleared and the next read will result in either an 'idle' message or an 'Error codes' message if not all required objects have been correctly set. If the read returned 'idle', a new file operation can now be started. Following are possible values returned as Error codes for file move: ■ 1 - atFilev2SourceDevice has not been set ■ 2 - atFilev2SourceFilename has not been set ■ 3 - atFilev2DestinationDevice has not been set ■ 4 - atFilev2DestinationFilename has not been set ■ 5 - either atFilev2SourceDevice or atFilev2DestinationDevice are set to TFTP ■ 6 - the combination of source device, stackID and filename is the same as the destination device, stackID and filename (i.e. it is not valid to move a file onto itself. Provided all above requirements are met, immediately upon executing the SNMP set, the device will indicate that it was a success. The actual file move itself will be started and continue on the device until it has completed. For large files, operations can take several minutes to complete. Subsequent reads of the object will return one of messages shown in the first table, to allow for tracking of the progress of the move operation.

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2DeleteBegin	{ atFilev2Operation 9 }	Represents the status of the delete file operation, in the form of octet string. A read on this object can return several possible values, depending on the current status of the system and the various file operation objects: ■ idle - There is no file operation in progress and all required objects have been set correctly. Setting a '1' to this object will begin the file deletion. ■ Error codes: [1-3] - A delete operation cannot be started until these errors are resolved. See below for key. ■ [action]ing x [--> y] - A file operation is currently in progress. You cannot start another operation while the object is returning this value. ■ [action] x [--> y] success - The last copy, move or delete operation was successfully completed. ■ [action] x [--> y] failure: [err] - The last copy, move or delete operation failed, with the error message attached. Common failures include lack of space on the destination file system, incorrect source file names or communication errors with remote services. Upon reading a success or failure message, the message will be cleared and the next read will result in either an 'idle' message or an 'Error codes' message if not all required objects have been correctly set. If the read returned 'idle', a new file operation can be started. File deletion operations ignore the values set in the atFilev2DestinationStackID, atFilev2DestinationDevice and atFilev2DestinationFilename objects. The file deletion operation is equivalent to the CLI 'delete force [file]' command, so it is possible to delete any normally-protected system files, such as the currently configured boot release. Following are possible values returned as Error codes for file move: ■ 1 - atFilev2SourceDevice has not been set ■ 2 - atFilev2SourceFilename has not been set ■ 3 - atFilev2SourceDevicehas not been set to TFTP Provided all above requirements are met, immediately upon executing the SNMP set, the device will indicate that it was a success. The actual file move itself will be started and continue on the device until it has completed. For large files, operations can take several minutes to complete. Subsequent reads of the object will return one of messages shown in the first table, to allow for tracking of the progress of the move operation.
atFilev2Flash_1	{ atFilev2Operation 10 }	Represents the Flash operation device object
atFilev2Card_2	{ atFilev2Operation 11 }	Represents the Card operation device object
atFilev2Nvs_3	{ atFilev2Operation 12 }	Represents the NVS operation device object
atFilev2Tftp_4	{ atFilev2Operation 13 }	Represents the TFTP operation device object
atFilev2TftpIPAddr	{ atFilev2Tftp_4 1 }	The IP address of the TFTP server that is to be used for the file copy process. This IP Address needs to be reachable from the device, or the file copy will fail.

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2Usb	{ atFilev2Operation 15 }	Represents the USB storage device operation device object.
atFilev2InfoEntry	{ atFilev2InfoTable 1 }	An entry in the list of files, containing information about a single file.
atFilev2InfoFilepath	{ atFilev2InfoEntry 1 }	The full path and name of the file. Files are sorted in alphabetical order and any filepath that is longer than 112 characters will not be displayed due to SNMP Object Identifier length limitations.
atFilev2InfoFileSize	{ atFilev2InfoEntry 2 }	The size of the file in bytes.
atFilev2InfoFileCreationTime	{ atFilev2InfoEntry 3 }	File creation time in the form <MMM DD YYYY HH:MM:SS>. For example, Sep 7 2008 06:07:54.
atFilev2InfoFileIsDirectory	{ atFilev2InfoEntry 4 }	This object will return the value TRUE if the entry is a directory, or FALSE if it is not.
atFilev2InfoFileIsReadable	{ atFilev2InfoEntry 5 }	This object will return the value TRUE if the file is readable, or FALSE if it is not.
atFilev2InfoFileIsWriteable	{ atFilev2InfoEntry 6 }	This object will return the value TRUE if the file is writeable, or FALSE if it is not.
atFilev2InfoFileIsExecutable	{ atFilev2InfoEntry 7 }	This object will return the value TRUE if the file is executable, or FALSE if it is not.
atFilev2USBMediaTable	{ atFilev2 6 }	The USB storage device table, containing information related to USB storage devices.
atFilev2USBMediaEntry	{ atFilev2USBMediaTable 1 }	Data pertaining to a USB storage device instance.
atFilev2USBMediaStackMemberId	{ atFilev2USBMediaEntry 1 }	The index of the stack member hosting this USB media. For devices that are not capable of being stacked, this object will always return the value 1.
atFilev2USBMediaPresence	{ atFilev2USBMediaEntry 2 }	This object indicates whether or not a USB storage device is inserted in a slot. Possible values are: ■ notPresent (1) ■ present (2)
atFilev2FileViewerStackId	atFilev2FileViewer 1	The stack ID of the stack member for which files will be displayed in the FileViewer table. For devices that are not capable of being stacked, this variable will always read as 1, and will cause an error on being written to with any value other than 1. Write this variable with the stack ID of the stack member for which a view of files is required. If the stack member doesn't exist, an error will be returned. For a chassis switch, it corresponds to the card ID. Note that the other variables specifying the files to view will not be altered by changing the stack ID, which means that the file view table could be empty if a non-existant device or path has been referenced previously.

Table 68-9: Objects defined in AT-FILEv2-MIB(cont.)

Object(cont.)	Object Identifier	Description
atFilev2FileViewerDevice	atFilev2FileViewer 2	The file system device for which files will be displayed in the FileViewer table. The values supported for this variable are identical to the values for other variables in the MIB, although not all values will actually result in the display of files. The different devices and whether they will result in the display of files are: ■ 1 - Flash - Onboard Flash - supported ■ 2 - Card - Removable SD card - supported ■ 3 - NVS - Onboard battery backed RAM - supported ■ 4 - FTP - not supported ■ 5 - USB - Removable USB media - supported Setting this variable to a unsupported value will result in an error, but setting to a value that is supported but on a device that doesn't contain that type of device will not. However, no files will be displayed in the File Viewer table in this case.
atFilev2FileViewerCurrentPath	atFilev2FileViewer 3	The file system path for which files will be displayed in the FileViewer table. This path will always read as a full pathname starting with the '/' character. Setting this variable will specify a new directory for which files will be displayed. The path specified must be the full path, relative setting of path does not work. Only paths with invalid characters in them will cause an error, paths specifying non-existent directories will be accepted, but no files will be displayed in the File Viewer table in this case.
atFilev2FileViewerTable	atFilev2FileViewer 4	A list of all files, not including pathnames, that are present on the device specified by atFilev2FileViewerStackId and atFilev2FileViewerDevice, in the path specified by atFilev2FileViewerCurrentPath. Hidden and system files are not displayed. If the Stack ID, device and path are invalid (the path is for a non-existent directory), the table will be empty. This will allow an MIB walk through the table even though the setup parameters are incorrect.
atFilev2FileViewerEntry	atFilev2FileViewerTable 1	An entry in the list of files, containing information about a single file.
atFilev2FileViewerName	atFilev2FileViewerEntry 1	The name of the file. Files are sorted in alphabetical order, and any name that is longer than 112 characters will not be displayed due to SNMP OID length limitations.
atFilev2FileViewerSize	atFilev2FileViewerEntry 2	The size of the file in bytes.
atFilev2FileViewerCreationTime	atFilev2FileViewerEntry 3	File creation time in the form <MMM DD YYYY HH:MM:SS>. For example, Sep 7 2008 06:07:54.
atFilev2FileViewerIsDirectory	atFilev2FileViewerEntry 4	Returns TRUE if the entry is a directory, FALSE otherwise.
atFilev2FileViewerIsReadable	atFilev2FileViewerEntry 5	Returns TRUE if the file is readable, FALSE otherwise.
atFilev2FileViewerIsWriteable	atFilev2FileViewerEntry 6	Returns TRUE if the file is writeable, FALSE otherwise.
atFilev2FileViewerIsExecutable	atFilev2FileViewerEntry 7	Returns TRUE if the file is executable, FALSE otherwise.

AT-IP-MIB

This MIB contains objects for Allied Telesis specific IP address management (**Table 68-10**). The objects reside in the module atIpMib { modules 602 }.

Table 68-10: Objects defined in AT-IP-MIB

Object	Object Identifier	Description
atIpMib	{ modules 602 }	MIB containing objects for IP addressing management.
AtIpAddressAssignmentType	Textual Convention	Object containing conditional coded values for the IP address assignment type being applied to the interface, referred to by objects in this MIB. The possible values and explanation are: ■ notSet (0) - indicates that the IP address assignment type has not yet been configured. This value can only ever be read. ■ primary (1) - indicates that the address is a primary IP address; only one primary address is allowed per interface. ■ secondary (2) - indicates that the address is a secondary IP address; any number of secondary IP addresses may be applied
AtIpAddressTable	{ atIpMib 1 }	A table containing mappings between primary or secondary IP addresses, and the interfaces they are assigned to. Indexed by: ■ atIpAddressAddrType ■ atIpAddressAddr
AtIpAddressEntry	{ AtIpAddressTable 1 }	Information about the address mapping for a particular interface.
atIpAddressAddrType	{ AtIpAddressEntry 1 }	An indication of the IP version of 'atIpAddressAddr'
atIpAddressAddr	{ AtIpAddressEntry 2 }	The IP address to which this entry's addressing information pertains. The address type of this object is specified in object 'atIpAddressAddrType'.
atIpAddressPrefixLen	{ AtIpAddressEntry 3 }	An integer, specifying the prefix length of the IP address represented by this entry.
atIpAddressLabel	{ AtIpAddressEntry 4 }	The name assigned to the IP address represented by this entry.
atIpAddressIfIndex	{ AtIpAddressEntry 5 }	The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index corresponds to the interface identified by the same value of the IF-MIB's ifIndex.
atIpAddressAssignmentType	{ AtIpAddressEntry 6 }	The IP address assignment type for this entry (primary or secondary), as described in the Textual Convention 'AtIpAddressAssignmentType'.

Table 68-10: Objects defined in AT-IP-MIB(cont.)

Object	Object Identifier	Description
atIpAddressRowStatus	{ AtIpAddressEntry 7 }	The current status of the IP address entry. The following values may be returned when reading this object: ■ active (1) « The IP address is currently mapped to an interface and is valid. ■ notReady (3) « The IP address is currently partially configured and is not mapped to an interface. The following values may be written to this object: ■ active (1) « An attempt will be made to map the IP address to the configured interface. ■ createAndWait (5) « An attempt will be made to create a new IP address entry. ■ destroy (6) « The IP address setting will be removed from the device. An entry cannot be made active until its atIpAddressPrefixLen, atIpAddressIfIndex and atIpAddressAssignmentType objects have been set to valid values.

AT-LICENSE-MIB

The AT-LICENSE-MIB contains objects for managing the AlliedWare Plus™ Operating System software licenses: listing applied software licenses, adding new licenses and deleting existing licenses (**Table 68-11**). The objects reside in the module license { sysinfo 22 }, organized in the following groups:

- Base Software License Table - a table containing the installed base software licenses on the device
- Installed Software License Table - a list of installed software licenses; used also to remove software license from the device
- Available Software Features Table
- LicenseNew - Objects used to install a new license
- LicenseStackRemove - Objects used to remove a license across a stack of devices

Table 68-11: Objects defined in AT-LICENSE-MIB

Object	Object Identifier	Description
license	{ sysinfo 22 }	MIB containing objects for listing applied software licenses, adding new licenses, and deleting existing licenses.
baseLicenseTable	{ license 1 }	Table containing information about base software licenses installed on a device. Indexed by: ■ baseLicenseStkId
baseLicenseEntry	{ baseLicenseTable 1 }	Information about a single license installed on the device.
baseLicenseStkId	{ baseLicenseEntry 1 }	The stack member ID of the device hosting the license.
baseLicenseName	{ baseLicenseEntry 2 }	The name of the base license.
baseLicenseQuantity	{ baseLicenseEntry 3 }	The number of licenses issued for this entry.
baseLicenseType	{ baseLicenseEntry 4 }	The type of base license issued.
baseLicenseIssueDate	{ baseLicenseEntry 5 }	The date of issue of the base license.
baseLicenseExpiryDate	{ baseLicenseEntry 6 }	The expiry date of the base license.
baseLicenseFeatures	{ baseLicenseEntry 7 }	The feature set that this license enables, in the format of an octet string. Each bit in the returned octet string represents a particular feature that can be license-enabled. The bit position within the string maps to the feature entry with the same index, in licenseFeatureTable. A binary '1' indicates that the feature is included in the license; a binary '0' indicates that the feature is not included in the license.
licenseTable	{ license 2 }	Table containing information about software licenses installed on the device. Indexed by: ■ licenseStackId ■ licenseIndex
licenseEntry	{ licenseTable 1 }	Information about a single installed software license on the device.
licenseStackId	{ licenseEntry 1 }	The stack member ID of the device hosting the license.
licenseIndex	{ licenseEntry 2 }	The index number of the license entry.
licenseName	{ licenseEntry 3 }	The name of the license.
licenseCustomer	{ licenseEntry 4 }	The name of the customer of the license.

Table 68-11: Objects defined in AT-LICENSE-MIB(cont.)

Object	Object Identifier	Description
licenseQuantity	{ licenseEntry 5 }	The number of licenses issued for this entry.
licenseType	{ licenseEntry 6 }	The type of license issued.
licenseIssueDate	{ licenseEntry 7 }	The date of issue of the license.
licenseExpiryDate	{ licenseEntry 8 }	The expiry date of the license.
licenseFeatures	{ licenseEntry 9 }	The feature set that this license enables, in the format of octet string. Each bit in the returned octet string represents a particular feature that can be license-enabled. The bit position within the string maps to the feature entry with the same index, in licenseFeatureTable. A binary '1' indicates that the feature is included in the license; a binary '0' indicates that the feature is not included in the license.
licenseRowStatus	{ licenseEntry 10 }	The current status of the license. The following values may be returned when reading this object: 1. active (1) - the license is currently installed and valid 2. notInService (2) - the license has expired or is invalid The following value may be written to this object: 3. destroy (6) - the license will be removed from the device; this may result in some features being disabled. Note that a stacked device that has a license deleted may not be able to rejoin the stack after reboot, unless the license is also deleted on all other devices in the stack.
licenseFeatureTable	{ license 3 }	Table containing all available Software Features. A feature must be license-enabled to be utilized on the device.
licenseFeatureEntry	{ licenseFeatureTable 1 }	Information about a single feature that must be license-enabled in order to be utilized on the device.
licenseFeatureIndex	{ licenseFeatureEntry 1 }	The index number of the feature which must be license-enabled.
licenseFeatureName	{ licenseFeatureEntry 2 }	The name of the feature under licensing control.
licenseFeatureStkMembers	{ licenseFeatureEntry 3 }	The set of stack members on which the feature is enabled, in the format of an octet string. Each bit in the string maps to an individual stacking member, e.g. bit one represents stacking member one, bit two represents stacking member two. A bit value of '1' indicates that the applicable feature is enabled on the matching device; a bit value of '0' indicates that the feature is disabled.
licenseNew	{ license 4 }	Group of objects available for updates, used when installing a new software license on the device.
licenseNewStackId	{ licenseNew 1 }	The ID of the stacking member upon which the new license is to be installed. The value zero (0) indicates that the license should be applied to all stack members.
licenseNewName	{ licenseNew 2 }	The name of the new license to be installed.
licenseNewKey	{ licenseNew 3 }	The key for the new license to be installed.

Table 68-11: Objects defined in AT-LICENSE-MIB(cont.)

Object	Object Identifier	Description
licenseNewInstall	{ licenseNew 4 }	Used to install new licenses. Values can be: 1. true (1) 2. false (2) To commence installation, a valid license name and key must first have been set via the licenseNewName and licenseNewKey respectively. This object should then be set to the value true (1). If either the license name or key is invalid, the write operation will fail. Once installed, the software modules affected by any newly enabled features will automatically be restarted. Note that a stacked device that has a new license installed on it may not be able to rejoin the stack after reboot, unless the license is also added to all other devices in the stack. When read, the object will always return the value false (2).
licenseNewInstallStatus	{ licenseNew 5 }	The current status of the last license installation request. One of the following values is returned when reading this object: ■ idle (1) ■ processing (2) ■ success (3) ■ failed (4) When a stack license installation operation is complete the first read of this object will return either a success (3) or a failure (4) indication. Subsequent reads of this object will then return an idle (1) indication.
licenseStackRemove	{ license 5 }	Group of objects used when removing a software license across a stack of devices.
licenseStackRemoveName	{ licenseStackRemove 1 }	The name of the license to be removed from all devices across the stack, on which the license currently exists.
licenseStackRemoveExecute	{ licenseStackRemove 2 }	When set to the value true (1), the system will attempt to remove the named license from all devices across the stack on which the license currently exists. All devices in a stack must be from the same product family and the named license must activate the same feature set on all devices.
licenseStackRemoveStatus	{ licenseStackRemove 3 }	The current status of the last requested stack license removal request. One of the following values is returned when reading this object: ■ idle (1) ■ processing (2) ■ success (3) ■ failed (4) When a stack license removal operation is complete the first read of this object will return either a success (3) or failure (4) indication. Subsequent reads of this object will then return an idle (1) indication.

AT-LOG-MIB

The AT Log MIB contains objects for listing log entries from the buffered and permanent logs (**Table 68-12**). The objects reside in the module log { modules 601 }, organized in the following groups:

- Log Table - objects containing the information from log messages issued by the system, ordered from oldest to newest entry
- Log Options - contains objects used to set up the log options configuration

Table 68-12: Objects defined in AT-LOG-MIB

Object	Object Identifier	Description
log	{ modules 601 }	MIB containing objects for listing log entries from the buffered and permanent logs.
logTable	{ log 1 }	A list of log entries from the source specified in the 'logSource' object. The list is ordered from oldest entry to newest entry. Indexed by: ■ logIndex
logEntry	{ logTable 1 }	Information about a single log entry, from the source specified in the 'logSource' object.
logIndex	{ logEntry 1 }	An index integer. This index is not directly tied to any specific log entry. Over time, the log will grow larger and eventually older entries will be removed from the log.
logDate	{ logEntry 2 }	The date of the log entry. Data resides in the format octet string, in the form YYYY MMM DD, e.g. 2008 Oct 9.
logTime	{ logEntry 3 }	The time of the log entry. Data resides in the format octet string, in the form HH:MM:SS, e.g. 07:15:04.
logFacility	{ logEntry 4 }	The syslog facility that generated the log entry, in the format octet string. See the reference manual for more information.
logSeverity	{ logEntry 5 }	The severity level of the log entry, in the format octet string. Severities are given below: ■ emerg Emergency, system is unusable ■ alert Action must be taken immediately ■ crit Critical conditions ■ errr Error conditions ■ warning Warning conditions ■ notice Normal, but significant, conditions ■ info Informational messages ■ debug Debug-level messages
logProgram	{ logEntry 6 }	The program that generated the log entry, in the format octet string. See the reference manual for more information.
logMessage	{ logEntry 7 }	The message of thew log entry, in the format octet string.
logOptions	{ log 2 }	Contains objects used to set up the required log options configuration.

Table 68-12: Objects defined in AT-LOG-MIB(cont.)

Object	Object Identifier	Description
logSource	{ logOptions 1 }	An integer indicating the source from which the log entries are retrieved. The valid values are: ■ 1 - Buffered log (default) ■ 2 - Permanent log. This information is used when retrieving the logTable objects, and also specifies the log to be cleared when the 'clearLog' object is set.
logAll	{ logOptions 2 }	An integer indicating whether to display all log entries in the logTable objects, or not. The valid values are: ■ 0 - to display only the most recent log messages. This is the default ■ 1 - to show all available log entries. Note: Choosing to display all log entries may result in delays of several seconds when accessing the logTable objects.
clearLog	{ logOptions 3 }	An integer indicating whether to clear the log that is specified by the 'logSource' object. Valid values are: ■ 0 - do not clear log ■ 1 - clear log

AT-LOOPPROTECT-MIB

The atLoopProtect-MIB (**Figure 68-5**, **Table 68-13**) defines objects for managing Loop Protection objects and triggers. Objects in this group have the object identifier atLoopProtect ({ modules 4 }).

Figure 68-5: The ATLoopProtect MIB Sub-tree

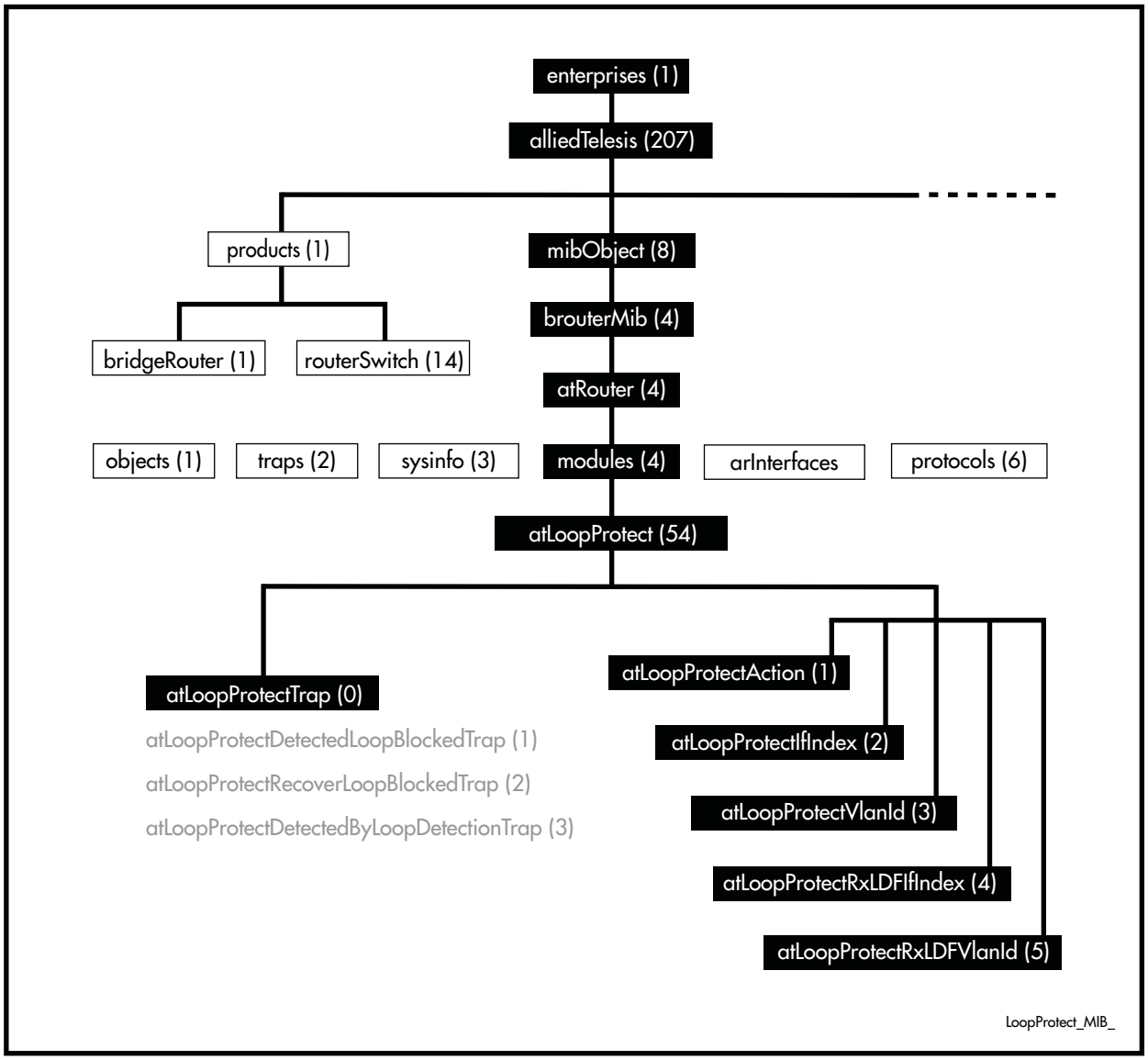


Table 68-13: Objects Defined in the AT-Loop Protect MIB

Object	Object Identifier	Description
{ atLoopProtect }	{ modules 54 }	The root of the Loop Protect object sub tree.
{ atLoopProtectTrap }	{ atLoopProtect0 }	The Loop Protection node state transition trap. List of traps (notifications) generated for Loop Protection.

Table 68-13: Objects Defined in the AT-Loop Protect MIB(cont.)

Object	Object Identifier	Description
{ atLoopProtectDetected LoopBlockedTrap }	{ atLoopProtectTrap1 }	Notification generated when the Loop Protection feature blocks an interface with a loop. The following bindings are associated with this trap: 1. atLoopProtectIfIndex 2. atLoopProtectVlanId 3. atLoopProtectAction
{ atLoopProtectRecover LoopBlockedTrap }	{ atLoopProtectTrap2 }	Notification generated when the Loop Protection feature restores a blocked interface back to normal operation. The following bindings are associated with this trap: 1. atLoopProtectIfIndex 2. atLoopProtectVlanId 3. atLoopProtectAction
{ atLoopProtectDetected ByLoopDetectionTrap }	{ atLoopProtectTrap3 }	Notification generated when the Loop Protection feature detects a loop by Loop Detection method. The following bindings are associated with this trap: 1. atLoopProtectIfIndex 2. atLoopProtectVlanId 3. atLoopProtectRxLDFIfIndex 4. atLoopProtectRxLDFVlanId
{ atLoopProtectAction }	{ atLoopProtect1 }	The Action for the Loop Protection feature. The following values are defined: 1. atLoopProtectAction-LearnDisable (0) 2. atLoopProtectAction-LearnEnable (1) 3. atLoopProtectAction-PortDisable (2) 4. atLoopProtectAction-PortEnable (3) 5. atLoopProtectAction-LinkDown (4) 6. atLoopProtectAction-LinkUp (5) 7. atLoopProtectAction-VlanDisable (6) 8. atLoopProtectAction-VlanEnable (7)
{ atLoopProtectIfIndex }	{ atLoopProtect2 }	The interface on which the loop was detected.
{ atLoopProtectVlanId }	{ atLoopProtect3 }	The VLAN ID on which the loop was detected.
{ atLoopProtectRxLDFIfIndex }	{ atLoopProtect4 }	The interface on which the loop detection frame was received.
{ atLoopProtectRxLDFVlanId }	{ atLoopProtect5 }	The VLAN ID on which the loop detection frame was received.

AT-MIBVERSION-MIB

The AT-MIBVERSION-MIB contains an object to display the last software release that contained changes to the supported AT Enterprise MIB definition files (**Table 68-14**). Objects in this group have the object identifier atMibsetVersion ({ sysinfo 15 }).

Table 68-14: Object defined in AT-MIBVERSION-MIB

Object	Object Identifier	Description
atMibVersion	{ sysinfo 15 }	This object returns a five digit integer which indicates the last software release that contained changes to the supported AT Enterprise MIB definition files. For example, If the currently loaded software release on the device is 5.3.1-0.3 but the Enterprise MIBs have not changed since 5.3.1-0.1, then the value returned will be 53101.

AT-NTP-MIB

This MIB contains objects for managing the Allied Telesis Network Time Protocol (NTP) configuration (**Table 68-15**). The objects reside in the module atNtp { modules 502 }, organized in the following groups:

- NTP Peer/Server Table - a table containing information on the Network Time Protocol (NTP) peers or server configurations in the system.
- Associations Table - a list of installed software; used also to remove software from the device.
- Status Table - Objects in this group are not supported.

Table 68-15: Objects defined in AT-NTP-MIB

Object	Object Identifier	Description
atNtp	{ modules 502 }	MIB containing objects for configuring NTP.
atNtpPeerIndexNext	{ atNtp 6 }	The next available index number to be used for object 'atNtpPeerIndex'.
atNtpPeerTable	{ atNtp 7 }	Table containing information on the Network Time Protocol (NTP) peers or server configurations in the system. Indexed by: ■ atNtpPeerIndex
atNtpPeerEntry	{ atNtpPeerTable 1 }	Information about a single NTP server or peer configuration.
atNtpPeerIndex	{ atNtpPeerEntry 1 }	The index number corresponding to a particular NTP server or peer configuration in the system. To create a new entry, the value of this object should be the same as that of the value of atNtpPeerIndexNext object, otherwise the entry creation will fail.
atNtpPeerNameAddr	{ atNtpPeerEntry 2 }	The host name, or the IP address of the NTP peer. When a new row (entry) is created, this object is set with a default of '0.0.0.0', and the management application should change it to a desired value by using a SET operation.
atNtpPeerMode	{ atNtpPeerEntry 3 }	The mode of the peer. Can be one of the following: ■ server (1) ■ peer (2) - default
atNtpPeerPreference	{ atNtpPeerEntry 4 }	The values in this object specifies whether this peer is the preferred one. Valid values are 0 to 2: ■ 0 - unknown - default ■ 1 - not preferred ■ 2 - preferred When the value is 'not preferred' (1) NTP chooses the peer with which to synchronize the time on the local system. If the object is set to 'preferred' (2) NTP will choose the corresponding peer to synchronize the time with.

Table 68-15: Objects defined in AT-NTP-MIB(cont.)

Object	Object Identifier	Description
atNtpPeerVersion	{ atNtpPeerEntry 5 }	The NTP version the peer supports. Can be one of the following: ■ 0 - unknown - default ■ 1 - version 1 ■ 2 - version 2 ■ 3 - version 3 ■ 4 - version 4
atNtpPeerKeyNumber	{ atNtpPeerEntry 6 }	The authentication key number. Default number is 0.
atNtpPeerRow Status	{ atNtpPeerEntry 7 }	The current status of this peer entry. The following values may be returned when reading this object: ■ active (1) - this value is returned on reading of this entry. ■ createAndGo (4) - this value is set by the management application when creating a new entry ■ destroy (6) - value set by the management application when deleting the entry. When an entry is deleted, all subsequent entries in the table will be re-indexed.
atNtpAssociationTable	{ atNtp 10 }	Table containing information on the Network Time Protocol (NTP) associations. Indexed by: ■ atNtpAssociationIndex
atNtpAssociationEntry	{ atNtpAssociationTable 1 }	Information about a single NTP server or peer configuration.
atNtpAssociationIndex	{ atNtpAssociationEntry 1 }	The index number corresponding to a particular NTP server or peer configuration in the system. To create a new entry, the value of this object should be the same as that of the value of atNtpPeerIndexNext object, otherwise the entry creation will fail.
atNtpAssociationPeerAddr	{ atNtpAssociationEntry 2 }	The host name, or the IP address of the NTP peer. When a new row (entry) is created, this object is set with a default of '0.0.0.0', and the management application should change it to a desired value by using a SET operation.
atNtpAssociationStatus	{ atNtpAssociationEntry 3 }	The status of this association. Can be one of the following: ■ master (synced) ■ master (unsynced) ■ selected ■ candidate ■ configured ■ unknown
atNtpAssociationConfigured	{ atNtpAssociationEntry 4 }	The value in this object specifies whether the association is from configuration or not. Value can be: ■ configured ■ dynamic
atNtpAssociationRefClkAddr	{ atNtpAssociationEntry 5 }	The IP Address for the reference clock.
atNtpAssociationStratum	{ atNtpAssociationEntry 6 }	The stratum of the peer clock.

Table 68-15: Objects defined in AT-NTP-MIB(cont.)

Object	Object Identifier	Description
atNtpAssociationPoll	{ atNtpAssociationEntry 7 }	The time between NTP requests from the device to the server, in seconds.
atNtpAssociationReach	{ atNtpAssociationEntry 8 }	An integer that indicates the reachability status of the peer.
atNtpAssociationDelay	{ atNtpAssociationEntry 9 }	The round trip delay between the device and the server.
atNtpAssociationOffset	{ atNtpAssociationEntry 10 }	The difference between the device clock and the server clock.
atNtpAssociationDisp	{ atNtpAssociationEntry 11 }	The lowest measure of error associated with peer offset, based on delay, in seconds.
atNtpStatus	{ atNtp 11 }	Group of objects containing system status information. The objects in this group are not supported.
atNtpSysClockSync	{ atNtpStatus 1 }	Not supported.
atNtpSysStratum	{ atNtpStatus 2 }	Not supported.
atNtpSysReference	{ atNtpStatus 3 }	Not supported.
atNtpSysFrequency	{ atNtpStatus 4 }	Not supported.
atNtpSysPrecision	{ atNtpStatus 5 }	Not supported.
atNtpSysRefTime	{ atNtpStatus 6 }	Not supported.
atNtpSysClkOffset	{ atNtpStatus 7 }	Not supported.
atNtpSysRootDelay	{ atNtpStatus 8 }	Not supported.
atNtpSysRootDisp	{ atNtpStatus 9 }	Not supported.

AT-PRODUCTS-MIB

AT-PRODUCT-MIB defines object identifiers for Allied Telesis products. Objects in this MIB have the object identifier products ({ alliedTelesis 1 }) OID 1.3.6.1.4.1.207.1.

Table 68-16 lists object identifiers for products supported by the AlliedWare Plus™ Operating System.

Table 68-16: Object identifiers for Allied Telesis products supported by the AlliedWare Plus™ Operating System

Object	Object Identifier	Description
products	{ alliedTelesis 1 }	
swhub	{ products 4 }	Subtree beneath which switching hubs are defined.
at_x200_GE52T	{ swhub 181 }	x200-GE52T layer two switch
at_x200_GE28T	{ swhub 182}	x200-GE28T layer two switch
at_x210_9GT	{ swhub 196}	x210-9GT, 8xGigbit, 1xSFP/T
at_x210_16GT	{ swhub 197}	x210-16GT, 14xGigbit, 2xcombo SFP/T
at_x210_24GT	{ swhub 198}	x210-24GT, 20xGigbit, 4xcombo SFP/T
at_x310_26FT	{ swhub 216}	AT-x310-26FT layer two switch with 24 10/100 Base-T ports, two 10/100/1000 Base-T ports, and four 10 Gb/s SFP+ ports.
at_x310_50FT	{ swhub 217}	AT-x310-50FT layer two switch with 48 10/100 Base-T ports, two 10/100/1000 Base-T ports, and four 10 Gb/s SFP+ ports.
at_x310_26FP	{ swhub 218}	AT-x310-26FP layer two switch with 24 10/100 Base-T ports, two 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports, plus PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
at_x310_50FP	{ swhub 219}	AT-x310-50FP layer two switch with 48 10/100 Base-T ports, two 10/100/1000 Base-T ports, four 10 Gb/s SFP+ ports, plus PSE function available on pins 1/2 and 3/6 (Mode A) of every copper port.
routerSwitch	{ products 14 }	Subtree beneath which router and (non industrial) switch product MIB object IDs are assigned.
at_SwitchBladex908	{ routerSwitch 69 }	Switchblade x908 8 Slot Layer 3 Switch Chassis
at_x900_12XTS	{ routerSwitch 70 }	AT-x900-12XT/S Advanced Gigabit Layer 3+ Expandable Switch, 12 x combo ports (10/100/1000BASE-T copper or SFP), 1 x 30Gbps expansion bay
at_x900_24XT	{ routerSwitch 75 }	x900-24XT Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays
at_x900_24XS	{ routerSwitch 76 }	x900-24XS Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays
at_x900_24XT_N	{ routerSwitch 77 }	x900-24XT-N Enhanced Gigabit Layer 3+ Expandable Switch, 24 x 10/100/1000BASE-T copper ports (RJ-45 connectors), 2 x 20 Gigabit expansion bays, NEBS compliant
at_x600_24Ts	{ routerSwitch 80 }	x600-24Ts Stackable Managed L2+/L3 Ethernet Switch, 24 x 1000BASE-T copper ports, 4 x SFP (combo) ports
at_x600_24TsXP	{ routerSwitch 81 }	x600-24Ts/XP Stackable Managed L2+/L3 Ethernet Switch, 24 x 1000BASE-T copper ports, 4 x SFP (combo) ports, 2 x XFP ports
at_x600_48Ts	{ routerSwitch 82 }	x600-48Ts Stackable Managed L2+/L3 Ethernet Switch, 48 x 1000BASE-T copper ports, 4 x SFP ports

Table 68-16: Object identifiers for Allied Telesis products supported by the AlliedWare Plus™ Operating

Object	Object Identifier	Description
at_x600_48TsXP	{ routerSwitch 83 }	x600-48Ts/XP Stackable Managed L2+/L3 Ethernet Switch, 48 x 1000BASE-T copper ports, 4 x SFP ports, 2 x XFP ports
at_x600-24TsPoE	{ routerSwitch 91}	x600-24Ts-POE Stackable Managed L2+/L3 Ethernet PoE Switch, 24 x 1000BASE-T PoE ports, 4 x SFP (combo) ports
at_x600_24TPoEPlus	{routerSwitch 92}	x600-24Ts-POE+ Stackable Managed L2+/L3 Ethernet PoE+ Switch, 24 x 1000BASE-T PoE+ ports, 4 x SFP (combo) ports
x610_48Ts_X_POEPlus	{routerSwitch 93}	x610-48Ts/X-POE+ Stackable Managed L2+/L3 Ethernet PoE+ Switch, 48 x 1000BASE-T PoE+ ports, 2 x SFP (combo) ports, 2 x SFP+ ports
x610_48Ts_POEPlus	{routerSwitch 94}	x610-48Ts-POE+ Stackable Managed L2+/L3 Ethernet PoE+ Switch, 48 x 1000BASE-T PoE+ ports, 4 x SFP (combo) ports
x610_24Ts_X_POEPlus	{routerSwitch 95}	x610-24Ts/X-POE+ Stackable Managed L2+/L3 Ethernet PoE+ Switch, 24 x 1000BASE-T PoE+ ports, 4 x SFP (combo) ports, 2 x SFP+ ports
x610_24Ts_POEPlus	{routerSwitch 96}	x610-24Ts-POE+ Stackable Managed L2+/L3 Ethernet PoE+ Switch, 24 x 1000BASE-T PoE+ ports, 4 x SFP (combo) ports
x610_48Ts_X	{routerSwitch 97}	x610-48Ts/X Stackable Managed L2+/L3 Ethernet Switch, 48 x 1000BASE-T copper ports, 2 x SFP (combo) ports, 2 x SFP+ ports
x610_48Ts	{routerSwitch 98}	x610-48Ts Stackable Managed L2+/L3 Ethernet Switch, 24 x 1000BASE-T copper ports, 4 x SFP (combo) ports
x610_24Ts_X	{routerSwitch 99}	x610-24Ts/X Stackable Managed L2+/L3 Ethernet Switch, 24 x 1000BASE-T copper ports, 4 x SFP (combo) ports, 2 x SFP+ ports
x610_24Ts	{routerSwitch 100}	x610-24Ts Stackable Managed L2+/L3 Ethernet Switch, 24 x 1000BASE-T copper ports, 4 x SFP (combo) ports
x610_24SP_X	{routerSwitch 101}	x610-24SP/X Stackable Managed L2+/L3 Ethernet Switch, 24 x SFP (combo) ports, 2 x SFP+ ports
x510_28GTX	{routerSwitch 109}	x510-28GTX Stackable Managed L2+/L3 Ethernet Switch with 24 x 10/100/1000 Base-T ports and 4 x 10 Gb/s SFP+ ports.
x510_28GPX	{routerSwitch 110}	x510-28GPX Stackable Managed L2+/L3 Ethernet Switch with 24 x 10/100/1000 Base-T ports with PoE, 4 x 10 Gb/s SFP+ ports.
x510_28GSX	{routerSwitch 111}	x510-28GSX Stackable Managed L2+/L3 Ethernet Switch with 24 x 100/1000 SFP ports and 4 x 10 Gb/s SFP+ ports.
x510_52GTX	{routerSwitch 112}	x510-52GTX Stackable Managed L2+/L3 Ethernet Switch with 48 x 10/100/1000 Base-T ports and 4 x 10 Gb/s SFP+ ports.
x510_52GPX	{routerSwitch 113}	x510-52GPX Stackable Managed L2+/L3 Ethernet Switch with 48 x 10/100/1000 Base-T ports with PoE, and 4 x 10 Gb/s SFP+ ports.
at-SBx8106	{routerSwitch 114}	AT-SBx8106, SwitchBlade x8106 chassis.
x510DP_52GTX	{routerSwitch 116}	x510DP-52GTX Stackable Managed L2+/L3 Ethernet Switch with 48 x 10/100/1000 Base-T ports and 4 x 10 Gb/s SFP+ ports.

Table 68-16: Object identifiers for Allied Telesis products supported by the AlliedWare Plus™ Operating

Object	Object Identifier	Description
IX5_28GPX	{routerSwitch 117}	IX5-28GPX Stackable Managed L2+ Ethernet Switch with 24 x 10/100/1000 Base-T ports with PoE, 4 x 10 Gb/s SFP+ ports.
industrialSwitch	{ products 24 }	Subtree beneath which industrial switch product MIB object IDs are assigned.
at_IE200_6GT	{industrialSwitch 1}	IE200-6GT L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports and 2 x SFP uplinks (100/1000X).
at_IE200_6GP	{industrialSwitch 2}	IE200-6GP L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports (with 802.3at PoE+) and 2 x SFP uplinks (100/1000X).
at_IE200_6GPW	{industrialSwitch 3}	IE200-6GPW L2+ managed industrial Switch with 4 x 10/100/1000T LAN ports (with 802.3at PoE+) and 2 x SFP uplinks (100/1000X) and 802.11bgn wireless.

AT-RESOURCE-MIB

The AT-RESOURCE-MIB contains objects for displaying system hardware resource and host information (**Table 68-17**). Objects in this group have the object identifier rsc ({ sysinfo 21 }).

Table 68-17: Objects defined in AT-RESOURCE-MIB

Object and OID	Description
resource { sysinfo 21 }	Contains objects for displaying system hardware resource and host information.
rscBoardTable { resource 1}	Table containing information about boards installed in a device. Indexed by: 1. rscStkId 2. rscResourceId
rscBoardEntry { rscBoardTable 1 }	Information about a single board installed in the device.
rscStkId { rscBoardEntry 1 }	The ID of the stack member. It is a number from 1 to 8, assigned to a stackable unit by the operating system when it is stacked. A default of 1 is given to a stand-alone unit.
rscResourceId { rscBoardEntry 2 }	The resource ID number of the board. It is a number assigned to a hardware resource when the operating system detects its existence. Can be a value in range 1 to 4294967294.
rscBoardType { rscBoardEntry 3 }	The type of board. Can be one of the following: 1. Base 2. Expansion 3. Fan module 4. PSU
rscBoardName { rscBoardEntry 4 }	The name of the board. Can be one of the following: 1. SwitchBlade x908 2. XEM-12S 3. AT-PWR05-AC
rscBoardId { rscBoardEntry 5 }	The ID number of the board. Its value is an Allied Telesis assigned number, such as 274 for the XEM-12S, or 255 for the AT-9924Ts.
rscBoardBay { rscBoardEntry 6 }	The board installation location. Its value can be Bay1, Bay2, PSU1. For a base board, it has a value of a single character space.
rscBoardRevision { rscBoardEntry 7 }	The revision number of the board.
rscBoardSerialNumber { rscBoardEntry 8 }	The serial number of the board.
hostInfoTable { resource 2 }	Table containing general system information. Indexed by rscStkId.
hostInfoEntry { hostInfoTable 1 }	Information about a single system parameter
hostInfoDRAM { hostInfoTable 2 }	The host DRAM information.
hostInfoFlash { hostInfoTable 3 }	The host Flash information.

Table 68-17: Objects defined in AT-RESOURCE-MIB(cont.)

Object and OID		Description
	hostInfoUptime { hostInfoTable 4 }	The host up-time.
	hostInfoBootloaderVersion { hostInfoTable 5 }	The host boot loader version.

AT-SETUP-MIB

AT-SETUP-MIB defines objects for managing software installation and configuration files (**Figure 68-6**, **Table 68-18**). Objects in this group have the object identifier setup ({ modules 500 }). The procedure in **Table 66-6 on page 66.22** shows how to use these MIB objects to upgrade to a new software version and boot configuration file. For objects used for file copying, see **"AT-FILEv2-MIB" on page 68.32**.

Figure 68-6: The AT-SETUP-MIB sub-tree

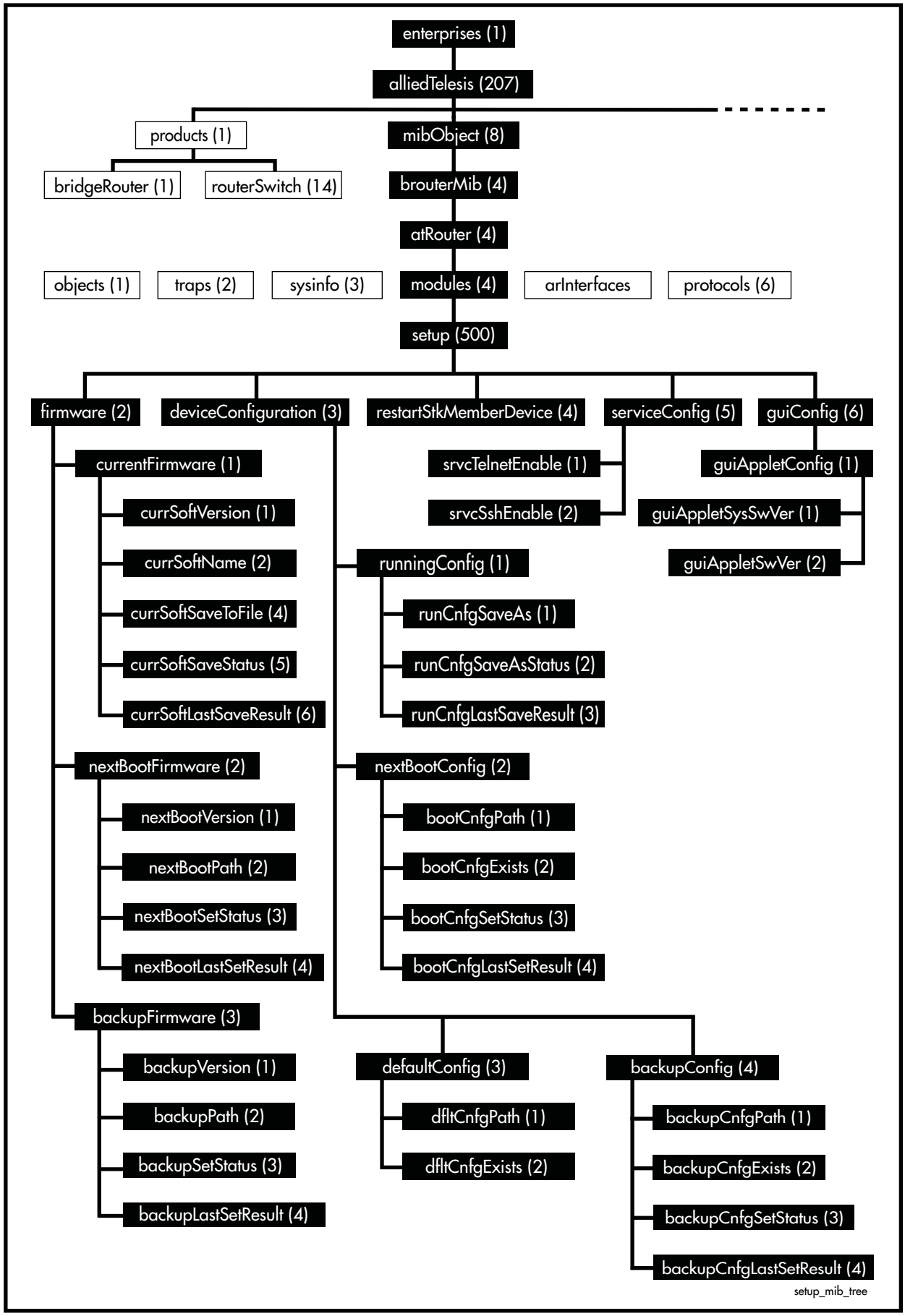


Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
restartDevice	{ setup 1 }	Object for restarting the device. When set to '1', the device will restart immediately. Note: This object has been deprecated. Use instead the restartStkMemberDevice object.
firmware	{ setup 2 }	Objects for managing the software version files that the device will install and run.
currentFirmware	{ firmware 1 }	Information about the current software version installed on the device.
currSoftVersion	{ currentFirmware 1 }	Current software version.
currSoftName	{ currentFirmware 2 }	Current software name.
currSoftSaveAs	{ currentFirmware 3 }	The file name to save the currently running software to the root of the Flash. Only one save operation can be executed at a time across all SNMP users. Note: This object has been deprecated. Use instead the currSoftSaveToFile, currSoftSaveStatus and currSoftLastSaveResult objects.
currSoftSaveToFile	{ currentFirmware 4 }	Set with a URL to save the currently running software to the root of Flash or USB flash drive (e.g. 'flash:/filename.rel' or 'USB:/filename.rel'). The URL must not contain whitespace characters. Only one save operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of currSoftSaveStatus is 'idle'. Immediately upon executing the set action, the actual firmware save operation is started and will continue on the device until it has completed or a failure occurs. When read, this object will return the URL of the last firmware save operation that was attempted.
currSoftSaveStatus	{ currentFirmware 5 }	This object will return the status of any current operation to store the running software to a release file. The following values may be returned: 1. (idle) - there is no release file save operation in progress 2. (success) - the last release file save operation completed successfully 3. (failure) - the last release file save operation failed 4. (saving) - a release file save operation is currently in progress When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading currSoftLastSaveResult.
currSoftLastSaveResult	{ currentFirmware 6 }	Gives an indication of the result of the last completed SNMP operation to save the running firmware to a release file.

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
nextBootFirmware	{ firmware 2 }	Information about the software version to be installed on the device when booting.
nextBootVersion	{ nextBootFirmware 1 }	Provides information on the software version (major.minor.interim, for example version 5.4.1) that the device will boot from. A zero will be returned if the version cannot be determined.
nextBootPath	{ nextBootFirmware 2 }	The full path to the release file that will be used the next time the device is rebooted. The URL must not contain whitespace characters. Only one set operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of nextBootSetStatus is 'idle'. Immediately upon executing the set action, the system will attempt to set the new configuration path, and the process will continue on the device until it has completed or a failure occurs. This object can be set with an empty string in order to clear the current boot firmware. Otherwise, the path should be of the form 'flash:/filename.cfg' or 'card:/filename.cfg'. In order to set this object, the file must meet the following conditions: ■ it must exist ■ it must be located in the root of Flash (on the active master in a stacked environment) or USB flash drive ■ it must not be the same as the backup release file ■ it must have a .rel suffix ■ it must pass several internal checks to ensure that it is a genuine release file ■ in a stacked environment, there must be enough disk space available to store the release file on each stack member
nextBootSetStatus	{ nextBootFirmware 3 }	Returns the status of any current operation to set the next boot release file. The following values may be returned: ■ 1 (idle) - there is no boot release setting operation in progress ■ 2 (success) - the last boot release setting operation completed successfully ■ 3 (failure) - the last boot release setting operation failed ■ 5 (syncing) - a boot release setting operation is currently in progress and the file is being synchronized across the stack When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading nextBootLastSetResult.
nextBootLastSetResult	{ nextBootFirmware 4 }	Gives an indication of the result of the last completed SNMP operation to set the boot release filename.

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
backupFirmware	{ firmware 3 }	Information about the backup software version and path.
backupVersion	{ backupFirmware 1 }	Provides information on the backup software version (major.minor.interim, for example version 5.4.1) that the device will boot from. A zero will be returned if the version cannot be determined.
backupPath	{ backupFirmware 2 }	The full path to the backup release file that will be used the next time the device is rebooted. The URL must not contain whitespace characters. Only one set operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of backupSetStatus is 'idle'. Immediately upon executing the set action, the system will attempt to set the new configuration path, and the process will continue on the device until it has completed or a failure occurs. This object can be set with an empty string in order to clear the current backup firmware. Otherwise, the path should be of the form 'flash:/filename.cfg' or 'card:/filename.cfg'. In order to set this object, the file must meet the following conditions: ■ it must exist ■ it must be located in the root of Flash (on the active master in a stacked environment) or USB flash drive ■ it must not be the same as the configured main release file ■ it must have a .rel suffix ■ it must pass several internal checks to ensure that it is a genuine release file ■ in a stacked environment, there must be enough disk space available to store the release file on each stack member
backupSetStatus	{ backupFirmware 3 }	Returns the status of any current operation to set the backup boot release file. The following values may be returned: ■ 1 (idle) - there is no backup boot release setting operation in progress ■ 2 (success) - the last backup boot release setting operation completed successfully ■ 3 (failure) - the last backup boot release setting operation failed ■ 5 (syncing) - a backup boot release setting operation is currently in progress and the file is being synchronized across the stack When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading backupLastSetResult.
backupLastSetResult	{ backupFirmware 4 }	Gives an indication of the result of the last completed SNMP operation to set the backup boot release filename.
deviceConfiguration	{ setup 3	Objects for managing device configuration.
runningConfig	{ deviceConfiguration 1 }	

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
runCnfgSaveAs	{ runningConfig 1 }	Set with a URL to save the currently running software to the root of Flash or USB flash drive (e.g. 'flash:/filename.rel' or 'usb:/filename.rel'). The URL must not contain whitespace characters. Only one set operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of runCnfgSaveAsStatus is 'idle'. Immediately upon executing the set action, the system will attempt to save the running configuration and the process will continue on the device until it has completed or a failure occurs. When read, this object will return the URL of the last firmware save operation that was attempted.
runCnfgSaveAsStatus	{ runningConfig 2 }	Returns the status of any current operation to save the running configuration. The following values may be returned: 1. (idle) - there is no config file save operation in progress 2. (success) - the last config file save operation completed successfully 3. (failure) - the last config file save operation failed 4. (saving) - a config file save operation is currently in progress When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading runCnfgLastSaveResult.
runCnfgLastSaveResult	{ runningConfig 3 }	Gives an indication of the result of the last completed SNMP operation to save the running configuration.
nextBootConfig	{ deviceConfiguration 2 }	
bootCnfgPath	{ nextBootConfig 1 }	The full path to the configuration file that will be used the next time the device is rebooted. The URL must not contain whitespace characters. Only one set operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of bootCnfgSetStatus is 'idle'. Immediately upon executing the set action, the system will attempt to set the new configuration path, and the process will continue on the device until it has completed or a failure occurs. This object can be set with an empty string in order to clear the current boot configuration. Otherwise, the path should be of the form 'flash:/myconfig.cfg' or 'card:/filename.cfg'. In order to set this object, the file must meet the following conditions: ■ it must exist ■ it must be located in the root of Flash (on the active master in a stacked environment) or USB flash drive ■ it must have a .cfg suffix ■ in a stacked environment, there must be enough disk space available to store the configuration file on each stack member

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
bootCnfgExists	{ nextBootConfig 2 }	This object will return the value TRUE if the currently defined boot configuration file exists, or FALSE if it does not.
bootCnfgSetStatus	{ nextBootConfig 3 }	Returns the status of any current operation to set the next boot configuration file. The following values may be returned: ■ 1 (idle) - there is no boot configuration setting operation in progress ■ 2 (success) - the last boot configuration setting operation completed successfully ■ 3 (failure) - the last boot configuration setting operation failed ■ 5 (syncing) - a boot configuration setting operation is currently in progress and the file is being synchronized across the stack When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading bootCnfgLastSetResult.
bootCnfgLastSetResult	{ nextBootConfig 4 }	Gives an indication of the result of the last completed SNMP operation to set the boot configuration filename.
defaultConfig	{ deviceConfiguration 3 }	
dfltCnfgPath	{ defaultConfig 1 }	The full path of the configuration file to use as backup when the device is rebooted. This object is not settable. The default configuration file is always 'flash:/default.cfg'.
dfltCnfgExists	{ defaultConfig 2 }	This object will return the value TRUE if the currently defined default configuration file exists, or FALSE if it does not.
backupConfig	{ deviceConfiguration 4 }	

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
backupCnfgPath	{ backupConfig 1 }	The full path to the backup configuration file that will be used the next time the device is rebooted. The URL must not contain whitespace characters. Only one set operation can be executed at a time across all SNMP users and an operation may not be started unless the current value of backupCnfgSetStatus is 'idle'. Immediately upon executing the set action, the system will attempt to set the new backup configuration path, and the process will continue on the device until it has completed or a failure occurs. This object can be set with an empty string in order to clear the current boot configuration. Otherwise, the path should be of the form 'flash:/myconfig.cfg' or 'card:/filename.cfg'. In order to set this object, the file must meet the following conditions: ■ it must exist ■ it must be located in the root of Flash (on the active master in a stacked environment) or USB flash drive ■ it must have a .cfg suffix ■ in a stacked environment, there must be enough disk space available to store the configuration file on each stack member
backupCnfgExists	{ backupConfig 2 }	This object will return the value TRUE if the currently defined backup configuration file exists, or FALSE if it does not.
backupCnfgSetStatus	{ backupConfig 3 }	Returns the status of any current operation to set the next backup boot configuration file. The following values may be returned: ■ 1 (idle) - there is no backup boot configuration setting operation in progress ■ 2 (success) - the last backup boot configuration setting operation completed successfully ■ 3 (failure) - the last backup boot configuration setting operation failed ■ 5 (syncing) - a backup boot configuration setting operation is currently in progress and the file is being synchronized across the stack When a read of this object returns a value of 'success' or 'failure', it will immediately be reset to 'idle' and a new operation may be initiated if desired. A detailed description of the last completed operation may be determined by reading backupCnfgLastSetResult.
backupCnfgLastSetResult	{ backupConfig 4 }	Gives an indication of the result of the last completed SNMP operation to set the backup boot configuration filename.

Table 68-18: Objects defined in AT-SETUP-MIB

Object Identifier	Description	Object Identifier
restartStkMemberDevice	{ setup 4 }	This object causes a specified device to restart immediately. The restart is initiated by setting its value to the device's stack member ID. Setting its value to zero will cause all devices in the stack, or a standalone device, to restart. Reading the object will always return zero.
serviceConfig	{ setup 5 }	
srvcTelnetEnable	{ serviceConfig 1 }	This object is used to either read or set the state of the telnet server on a device. Telnet can be enabled by setting the value of this object to 'enable(1)' or can be disabled by setting the value 'disable(2)'.
srvcSshEnable	{ serviceConfig 2 }	This object is used to either read or set the state of the SSH server on a device. SSH can be enabled by setting the value of this object to 'enable(1)' or can be disabled by setting the value 'disable(2)'.
guiConfig	{ setup 6 }	
guiAppletConfig	{ guiConfig 1 }	
guiAppletSysSwVer	{ guiAppletConfig 1 }	This object represents the system software release that the currently selected GUI applet was designed to run on. The system automatically searches for GUI applet files that reside in the root directory of the Flash memory, and selects the latest available file that is applicable to the currently running system software. This is the applet that will be uploaded to a user's web browser when they initiate the GUI.
	{ guiAppletConfig 2 }	This object represents the software version of the currently selected GUI applet. The system automatically searches for GUI applet files residing in the root directory of the Flash memory, and selects the latest available one that is applicable to the currently running system software. This is the applet that will be uploaded to a user's web browser when they initiate the GUI.

AT-SMI-MIB

AT-SMI-MIB defines the high-level structure and root objects of the Allied Telesis Enterprise MIB (**Table 68-19**). These objects are imported by other component MIBs of the Allied Telesis Enterprise MIB.

Table 68-19: AT Enterprise MIB - High Level Structure

Object	Object Identifier	Description
alliedTelesis	{ enterprises 207 } 1.3.6.1.4.1.207	Root of the Allied Telesis Enterprise MIB under the private(4) node defined in RFC1155-SMI.
products	{ alliedTelesis 1 } 1.3.6.1.4.1.207.1	Sub-tree of all product OIDs. Described in **"AT-PRODUCTS-MIB" on page 68.52**.
bridgeRouter	{ products 1 } 1.3.6.1.4.1.207.1.1	Sub-tree of bridge product MIB objects (not applicable for AlliedWare Plus).
routerSwitch	{ products 14 } 1.3.6.1.4.1.207.1.2	Sub-tree for all router and switch product MIB objects.
industrialSwitch	{ products 24 } 1.3.6.1.4.1.207.1.24	Sub-tree for industrial switch product MIB objects.
mibObject	{ alliedTelesis 8 } 1.3.6.1.4.1.207.8	Sub-tree for all managed objects.
brouterMib	{ mibObject 4 } 1.3.6.1.4.1.207.8.4	Sub-tree of objects for managing bridges, routers, and switches.
atRouter	{ brouterMib 4 } 1.3.6.1.4.1.207.8.4.4	Sub-tree of objects for managing multiprotocol routers and switches.
objects	{ atRouter 1 } 1.3.6.1.4.1.207.8.4.4.1	Sub-tree of OIDs for boards, releases, interface types, and chips.
traps	{ atRouter 2 } 1.3.6.1.4.1.207.8.4.4.2	Sub-tree for generic traps (not applicable for AlliedWare Plus).
sysinfo	{ atRouter 3 } 1.3.6.1.4.1.207.8.4.4.3	Sub-tree of objects describing general system information.
modules	{ atRouter 4 } 1.3.6.1.4.1.207.8.4.4.4	Sub-tree of objects for monitoring and managing software features.
arInterfaces	{ atRouter 5 } 1.3.6.1.4.1.207.8.4.4.5	Sub-tree of objects describing boards, slots and physical interfaces.
protocols	{ atRouter 6 } 1.3.6.1.4.1.207.8.4.4.6	Sub-tree of OIDs for protocols.
atAgents	{ atRouter 7 } 1.3.6.1.4.1.207.8.4.4.7	Sub-tree of objects describing variations from standards.

Table 68-20 lists the major modules of the AT-SMI-MIB grouped by their object identifiers. Note that this is also the order in which they are described in this chapter.

Table 68-20: AT-SMI-MIBs Listed by Object Group

MIB Section	OID	Description
AT-SMI-MIB		This section describes the structure of management information for the Allied Telesis Enterprise object, alliedTelesis { 1.3.6.1.4.1.207 }.
AT-PRODUCTS-MIB	1.3.6.1.4.1.207.1	Object identifiers for Allied Telesis products. See **"AT-PRODUCTS-MIB" on page 68.52**.

Table 68-20: AT-SMI-MIBs Listed by Object Group(cont.)

MIB Section	OID	Description
AT-BOARDS-MIB	1.3.6.1.4.1.207.8.4.4.1.1	Object identifiers for boards, interface types, and chip sets. See **"AT-BOARDS-MIB" on page 68.13**.
AT-SYSINFO-MIB	1.3.6.1.4.1.207.8.4.4.3	Objects that describe generic system information and environmental monitoring. See **"AT-SYSINFO-MIB" on page 68.68**.
AT-ENVMONv2-MIB	1.3.6.1.4.1.207.8.4.4.3.12	Objects and traps for monitoring fans, voltage rails, temperature sensors, and power supply bays. See **"AT-ENVMONv2-MIB" on page 68.21**.
AT-VCSTACK-MIB	1.3.6.1.4.1.207.8.4.4.3.13	Objects for managing Virtual Chassis Stacking (VCS). See **"AT-ENVMONv2-MIB" on page 68.21**.
AT-MIBVERSION-MIB	1.3.6.1.4.1.207.8.4.4.3.15	Object to display the last software release that contained changes to the support AT Enterprise MIB definition files. See **"AT-MIBVERSION-MIB" on page 68.48**.
AT-USER-MIB	1.3.6.1.4.1.207.8.4.4.3.20	Objects for displaying information of users currently logged into a device, or configured in the Local User Data base of the device. See **"AT-USER-MIB" on page 68.75**.
AT-RESOURCE-MIB	1.3.6.1.4.1.207.8.4.4.3.21	Objects for displaying system hardware resource information. See **"AT-RESOURCE-MIB" on page 68.55**.
AT-LICENSE-MIB	1.3.6.1.4.1.207.8.4.4.3.22	Objects for managing software licenses on devices using AlliedWare Plus™ Operating System. See **"AT-LICENSE-MIB" on page 68.41**.
AT-TRIGGER-MIB	1.3.6.1.4.1.207.8.4.4.4.53	Objects for managing triggers. See **"AT-TRIGGER-MIB" on page 68.73**.
AT-LOOPPROTECT-MIB	1.3.6.1.4.1.207.8.4.4.4.54	Objects for managing Allied Telesis Loop Protection. See **"AT-LOOPPROTECT-MIB" on page 68.46**.
AT-SETUP-MIB	1.3.6.1.4.1.207.8.4.4.4.500	Objects for managing software installation and configuration files. See **"AT-SETUP-MIB" on page 68.57**.
AT-DNS-CLIENT-MIB	1.3.6.1.4.1.207.8.4.4.4.501	Objects for managing Allied Telesis DNS Client Configuration. See **"AT-DNS-CLIENT-MIB" on page 68.20**.
AT-NTP-MIB	1.3.6.1.4.1.207.8.4.4.4.502	Objects for managing Allied Telesis Network Time Protocol (NTP) configuration. See **"AT-NTP-MIB" on page 68.49**.
AT-EPSRv2-MIB	1.3.6.1.4.1.207.8.4.4.4.536	Objects for managing Allied Telesis EPSR. See **"AT-EPSRv2-MIB" on page 68.29**.
AT-DHCPSN-MIB	1.3.6.1.4.1.207.8.4.4.4.537	Objects for managing Allied Telesis DHCP Snooping. See **"AT-DHCPSN-MIB" on page 68.17**.
AT-FILEv2-MIB	1.3.6.1.4.1.207.8.4.4.4.600	Objects for displaying and managing file content on local, stacked, and remote sources. See **"AT-FILEv2-MIB" on page 68.32**.
AT-LOG-MIB	1.3.6.1.4.1.207.8.4.4.4.601	Objects for listing log entries from the buffered and permanent logs. See **"AT-LOG-MIB" on page 68.44**.
AT-IP-MIB	1.3.6.1.4.1.207.8.4.4.4.602	Objects for Allied Telesis specific IP address management. See **"AT-IP-MIB" on page 68.39**.
AT-ALMMON-MIB	1.3.6.1.4.1.207.8.4.4.3.26	Objects for managing Allied Telesis Alarm Monitor.

AT-SYSINFO-MIB

AT-SYSINFO-MIB defines objects that describe generic system information and environmental monitoring. Objects in this group have the object identifier sysinfo ({ atRouter 3 }). **Table 68-21** lists the objects supported by the AlliedWare Plus™ sysinfo MIB.

Table 68-21: Objects defined in AT-SYSINFO-MIB

Object	Description
sysinfo { atRouter 3 } (1.3.6.1.4.1.207.8.4.4.3)	Subtree containing generic system information.
fanAndPs {sysinfo 1 } (1.3.6.1.4.1.207.8.4.4.3.1)	A collection of objects for monitoring fans and power supplies. For devices running the AlliedWare Plus™ Operating System, these objects are superceded by objects in the AT-ENVMON-MIB (see **"AT-ENVMONv2-MIB" on page 68.21**).
restartGroup {sysinfo 2 }	A collection of objects and traps for activating and monitoring restarts. This group is not supported by devices running the AlliedWare Plus™ Operating System.
cpu {sysinfo 3 }	A collection of objects containing information about the CPU utilization over different periods of time. All values are expressed as a percentage - integer in range 0 to 100.
cpuUtilisationMax {cpu 1 }	Maximum CPU utilization since the device was last restarted.
cpuUtilisationAvg {cpu 2 }	Average CPU utilization since the device was last restarted.
cpuUtilisationAvgLastMinute {cpu 3 }	Average CPU utilization over the past minute.
cpuUtilisationAvgLast10Seconds {cpu 4 }	Average CPU utilization over the past ten seconds.
cpuUtilisationAvgLastSecond {cpu 5 }	Average CPU utilization over the past second.
cpuUtilisationAvgMaxLast5Minutes {cpu 6 }	Maximum CPU utilization over the last 5 minutes.
cpuUtilisationAvgLast5Minutes {cpu 7 }	Average CPU utilization over the past 5 minutes.
cpuUtilisationStackTable {cpu 8 }	A list of stack members.
cpuUtilisationStackEntry {cpuUtilisationStackTable 1}	A set of parameters that describe the CPU utilization of a stack member
cpuUtilisationStackId {cpuUtilisationStackEntry 1}	Stack member ID.
cpuUtilisationStackMax {cpuUtilisationStackEntry 2}	Maximum CPU utilization since the router was last restarted. Expressed as a percentage.
cpuUtilisationStackAvg {cpuUtilisationStackEntry 3}	Average CPU utilization since the router was last restarted. Expressed as a percentage.
cpuUtilisationStackAvgLastMinute {cpuUtilisationStackEntry 4}	Average CPU utilisation over the past minute. Expressed as a percentage.

Table 68-21: Objects defined in AT-SYSINFO-MIB

Object	Description
cpuUtilisationStackAvgLast10Seconds {cpuUtilisationStackEntry 5}	Average CPU utilisation over the past ten seconds. Expressed as a percentage.
cpuUtilisationStackAvgLastSecond {cpuUtilisationStackEntry 6}	Average CPU utilisation over the past second. Expressed as a percentage.
cpuUtilisationStackMaxLast5Minutes {cpuUtilisationStackEntry 7}	Maximum CPU utilisation over the last 5 minutes. Expressed as a percentage.
cpuUtilisationStackAvgLast5Minutes {cpuUtilisationStackEntry 8}	Average CPU utilisation over the past 5 minutes. Expressed as a percentage.
sysTemperature {sysinfo 4 }	A collection of objects and traps for monitoring and managing the temperature status. For devices running the AlliedWare Plus™ Operating System.
atContactDetails {sysinfo 5 }	Contact details for Allied Telesis.
memory {sysinfo 7 }	A collection of objects and traps for monitoring memory usage and status.
atEnvMonv2 {sysinfo 12 }	AT Environment Monitoring v2 MIB for managing and reporting data relating to voltage rails, fan speeds, temperature sensors and power supply units. Objects under this portion of the OID are shown in the **"AT-ENVMONv2-MIB" on page 68.21**.
vcstack {sysinfo 13 }	A collection of objects for managing Virtual Chassis Stacking in AlliedWare Plus™. See **"AT-VCSTACK-MIB" on page 68.77**.
atPortInfo {sysinfo 14 }	Objects containing information about the transceiver of an interface. This portion of the object tree is documented separately in: **"AT-PORTINFO" on page 68.70**.
atVlanInfo {sysinfo 16 }	A collection of objects for counting bytes or incoming frames within a selected VLAN. Note that these objects are only appropriate for the IX5, x510 and x610 series products.
{sysinfo 17 } to {sysinfo 19 }	These objects are not supported on your switch.
user {sysinfo 20 }	Contains objects for displaying information of users currently logged into a device, or configured in its local database. Objects under this portion of the OID are shown in the **"AT-USER-MIB" on page 68.75**.
resource {sysinfo 21 }	Contains objects for displaying hardware resource information. Objects under this portion of the OID are shown in the **"AT-RESOURCE-MIB" on page 68.55**.
license {sysinfo 22 }	This MIB, is used for listing applied software licenses, adding new licenses, and deleting existing licenses. Objects under this portion of the OID are shown in the **"AT-LICENSE-MIB" on page 68.41**.
chassis {sysinfo 23 }	This MIB is used for accessing trap notifications on chassis based products. Note that these objects are only appropriate for the x8100 series products.

AT-PORTINFO

This table defines objects for managing interface port objects such as transceivers. Objects in this group have the object identifier atPortInfo ({ sysinfo 14 }), OID path, 1.3.6.1.4.1.207.8.4.4.3.14.

Table 68-22: Objects defined in AT-ATPORTINFO portion of the MIB

Object / Object Identifier	Description
atPortInfo {sysinfo 14}	This object returns information about interface transceivers.
atPortInfoTransceiverTable {atPortInfo 1}	A table of information about the transceiver of a interface.
atPortInfoTransceiverEntry {atPortInfoTransceiverTable 1}	The description, the transceiver type of a interface.
atPortInfoTransceiverifIndex {atPortInfoTransceiverEntry 1}	The ifIndex for the interface represented by this entry of the interfaces table.
atPortInfoTransceiverType {atPortInfoTransceiverEntry 2}	This object indicates the type of transceiver on a interface. It contains the following value list objects:

Table 68-22: Objects defined in AT-ATPORTINFO portion of the MIB(cont.)

Object / Object Identifier	Description
	The type of transceiver on an interface can be one of the following: ■ rj45(1) ■ sfp-px(2) ■ sfp-bx10(3) ■ sfp-fx(4) ■ sfp-100base-lx(5) ■ sfp-t(6) ■ sfp-cx(7) ■ sfp-zx-cwdm(8) ■ sfp-lx(9) ■ sfp-sx(10) ■ sfp-oc3-lr(11) ■ sfp-oc3-ir(12) ■ sfp-oc3-mm(13) ■ xfp-srsw(14) ■ xfp-lrlw(15) ■ xfp-erew(16) ■ xfp-sr(17) ■ xfp-lr(18) ■ xfp-er(19) ■ xfp-lrm(20) ■ xfp-sw(21) ■ xfp-lw(22) ■ xfp-ew(23) ■ unknown(24) ■ empty(25) ■ sfpp-sr(26) ■ sfpp-lr(27) ■ sfpp-er(28) ■ sfpp-lrm(29) ■ inf-1-x-copper-pasv(30) ■ inf-1-x-copper-actv(31) ■ inf-1-x-lx(32) ■ inf-1-x-sx(33) ■ cx4(34)

Table 68-22: Objects defined in AT-ATPORTINFO portion of the MIB(cont.)

Object / Object Identifier	Description
atPortRenumberEvents {atPortInfo 2}	The number of times that port number values (represented by the dot1dBasePort object in BRIDGE-MIB), have been re-assigned due to stack member leave/join events or XEM hot-swap events, since the system was initialized.

AT-TRIGGER-MIB

AT-TRIGGER-MIB defines objects for managing triggers (**Table 68-23**). Objects in this group have the object identifier trigger ({ modules 53 }). All objects in this group have read only access.

Table 68-23: Objects defined in AT-TRIGGER-MIB

Object Identifier	Description
triggerTraps { trigger 0 }	Sub-tree for all trigger traps.
triggerTrap { triggerTraps 1 }	Notification generated when a trigger is activated. It returns the value of triggerLastTriggerActivated.
triggerLastTriggerActivated { trigger 1 }	Trigger number of the most recent trigger activated on the switch.
triggerConfigInfoTable { trigger 9 }	Table of information about each trigger that has been configured, indexed by triggerNumber.
triggerConfigInfoEntry { triggerConfigInfoTable 1 }	Information about the configuration of a single trigger.
triggerNumber { triggerConfigInfoEntry 1 }	ID number of the trigger. Values are in range 1- 250.
triggerName { triggerConfigInfoEntry 2 }	Name and description of the trigger.
triggerTypeDetail { triggerConfigInfoEntry 3 }	Trigger type and its activation conditions.
triggerActiveDaysOrDate { triggerConfigInfoEntry 4 }	The days of a week or the date on which the trigger can be activated.
triggerActivateAfter { triggerConfigInfoEntry 5 }	Time after which the trigger can be activated.
triggerActivateBefore { triggerConfigInfoEntry 6 }	Time before which the trigger can be activated.
triggerActiveStatus { triggerConfigInfoEntry 7 }	Whether or not the trigger can be activated.
triggerTestMode { triggerConfigInfoEntry 8 }	Whether or not the trigger is operating in diagnostic (test) mode.
triggerSnmpTrap { triggerConfigInfoEntry 9 }	Whether or a not an SNMP trap will be generated when the trigger is activated.
triggerRepeatTimes { triggerConfigInfoEntry 10 }	Whether the trigger can repeat an unlimited number of times (continuous) or a specified number of times. If the trigger can repeat only a specified number of times, then the number of times the trigger has already been activated is displayed in brackets.
triggerLasttimeModified { triggerConfigInfoEntry 11 }	Date and time that the trigger configuration was last modified.
triggerNumberOfActivation { triggerConfigInfoEntry 12 }	Number of times the trigger has been activated since the last restart of the device.
triggerLasttimeActivation { triggerConfigInfoEntry 13 }	Date and time that the trigger was last activated.
triggerNumberOfScripts { triggerConfigInfoEntry 14 }	Number of scripts that this trigger will execute. Values are in range 0-5.

Table 68-23: Objects defined in AT-TRIGGER-MIB(cont.)

Object Identifier	Description
triggerScript1 { triggerConfigInfoEntry 15 }	Name of the first script that this trigger will execute if the trigger is activated.
triggerScript2 { triggerConfigInfoEntry 16 }	Name of the second script that this trigger will execute if the trigger is activated.
triggerScript3 { triggerConfigInfoEntry 17 }	Name of the third script that this trigger will execute if the trigger is activated.
triggerScript4 { triggerConfigInfoEntry 18 }	Name of the fourth script that this trigger will execute if the trigger is activated.
triggerScript5 { triggerConfigInfoEntry 19 }	Name of the fifth script that this trigger will execute if the trigger is activated.
triggerCounters { trigger 10 }	Collection of counters for trigger activations.
triggerNumOfActivation { triggerCounters 1 }	Number of times a trigger has been activated.
triggerNumOfActivationToday { triggerCounters 2 }	Number of times a trigger has been activated today.
triggerNumOfPerodicActivationToday { triggerCounters 3 }	Number of times a periodic trigger has been activated today.
triggerNumOfInterfaceActivationToday { triggerCounters 4 }	Number of times an interface trigger has been activated today.
triggerNumOfResourceActivationToday { triggerCounters 5 }	Number of times a CPU or memory trigger has been activated today.
triggerNumOfRebootActivationToday { triggerCounters 6 }	Number of times a reboot trigger has been activated today.
triggerNumOfPingPollActivationToday { triggerCounters 7 }	Number of times a ping-poll trigger has been activated today.
triggerNumOfStackMasterFailActivationToday { triggerCounters 8 }	Number of times a stack master fail trigger has been activated today.
triggerNumOfStackMemberActivationToday { triggerCounters 9 }	Number of times a stack member trigger has been activated today.

AT-USER-MIB

The AT-USER-MIB contains objects for displaying information about users currently logged into a device, or configured in the Local User Database of the device (**Table 68-24**). Objects in this group have the object identifier user ({ sysinfo 20 }).

Table 68-24: Objects defined in AT-USER-MIB

Object	Object Identifier	Description
userInfoTable (207.8.4.4.3.20.1)	{ user 1 }	Table containing information about users. Each entry in the table represents a user currently logged into the device. Indexed by: rscBoardType and rscBoardIndex.
userInfoEntry	{ userInfoTable 1 }	Information about a single user logged into the device.
userInfoType	{ userInfoEntry 1 }	The type of connection through which the user logged into the device. Can be: 1. console (1) 2. aux (2) 3. telnet (3) 4. script (4) 5. stack (5)
userInfoIndex	{ userInfoEntry 2 }	Index of the line upon which the user logged into the device. Can be a value in range 1 to 16.
userInfoName	{ userInfoEntry 3 }	User name of the user logged into the device.
userInfoPrivilegeLevel	{ userInfoEntry 4 }	The user's privilege level. Can be a value in range 1 to 15.
userInfoIdleTime	{ userInfoEntry 5 }	The amount of time since the user was last active, in the form hh:mm:ss.
userInfoLocation	{ userInfoEntry 6 }	The user location or login method. It can be an IP Address used by the user to telnet into the device, or an asyn port.
userInfoPasswordLifetime	{ userInfoEntry 7 }	The number of days remaining until the user's password expires. Depending on the current user setting it will display one of the following: No Expiry - the password will never expire (default setting) x days - where x is the remaining lifetime of the current password (maximum lifetime value is 1000 days) -x days (expired) - indicating that the current password expired x days ago
userInfoPasswordLastChange	{ userInfoEntry 8 }	The number of days since the password was last altered.

Table 68-24: Objects defined in AT-USER-MIB(cont.)

Object	Object Identifier	Description
userConfigTable	{ user 2 } or (207.8.4.4.3.20.2)	Table containing user configuration information. Each entry in the table relates to a user configured in the Local User Database of the device. Indexed by userConfigIndex.
userConfigEntry	{ userConfigTable 1 }	Information about a single user configured in the Local User Database of the device.
userConfigIndex	{ userConfigEntry 1 }	Unique number used to identify entries in the userConfigTable.
userConfigName	{ userConfigEntry 2 }	The user's name.
userConfigPrivilegeLevel	{ userConfigEntry 3 }	The privilege level granted to the user. Can be a value in range 1 to 15.
userSecurityPasswordRules	{ user 3 } or (207.8.4.4.3.20.3)	Information about user password security rules.
userSecurityPasswordHistory	{ userSecurityPasswordRules 1 }	The number of previous passwords that are retained for comparison when a user password is created. A new password must be unique when compared against the previous history. A value of 0 represents no restriction. The maximum number of retained passwords is 15.
userSecurityPasswordLifetime	{ userSecurityPasswordRules 2 }	The maximum number of days that the password may persist before a change is required. 0 means no expiry. The maximum value is 1000.
userSecurityPasswordWarning	{ userSecurityPasswordRules 3 }	The number of days before the password expires that a warning message is displayed when the user logs in. A value of 0 indicates no warning. The maximum value is 1000 but must always be less than the password lifetime.
userSecurityPasswordMinLength	{ userSecurityPasswordRules 4 }	The minimum allowable password length.
userSecurityPasswordMinCategory	{ userSecurityPasswordRules 5 }	The minimum number of different categories that the password must satisfy to be considered valid. Categories are split into four groups: upper-case letters lower-case letters digits special symbols. ASCII characters not included in the previous three categories.
userSecurityPasswordForced	{ userSecurityPasswordRules 6 }	Whether or not a user with an expired password is forced to change their password at the next login. At login a user with an expired password is prompted to change their password. If the new password meets the current security password rules the user is allowed to log in, otherwise they are rejected.
userSecurityPasswordReject	{ userSecurityPasswordRules 7 }	Whether or not a user login attempt with an expired password is rejected. If the user is not rejected then they can log in.

AT-VCSTACK-MIB

AT-VCSTACK-MIB defines objects for managing Virtual Chassis Stacking (**Table 68-25**). Objects in this group have the object identifier vcstack ({ sysinfo 13 }).

Figure 68-7 on page 68.77 shows the tree structure of the AT-VCSTACK objects.

Figure 68-7: The AT-VCSTACK MIB sub-tree

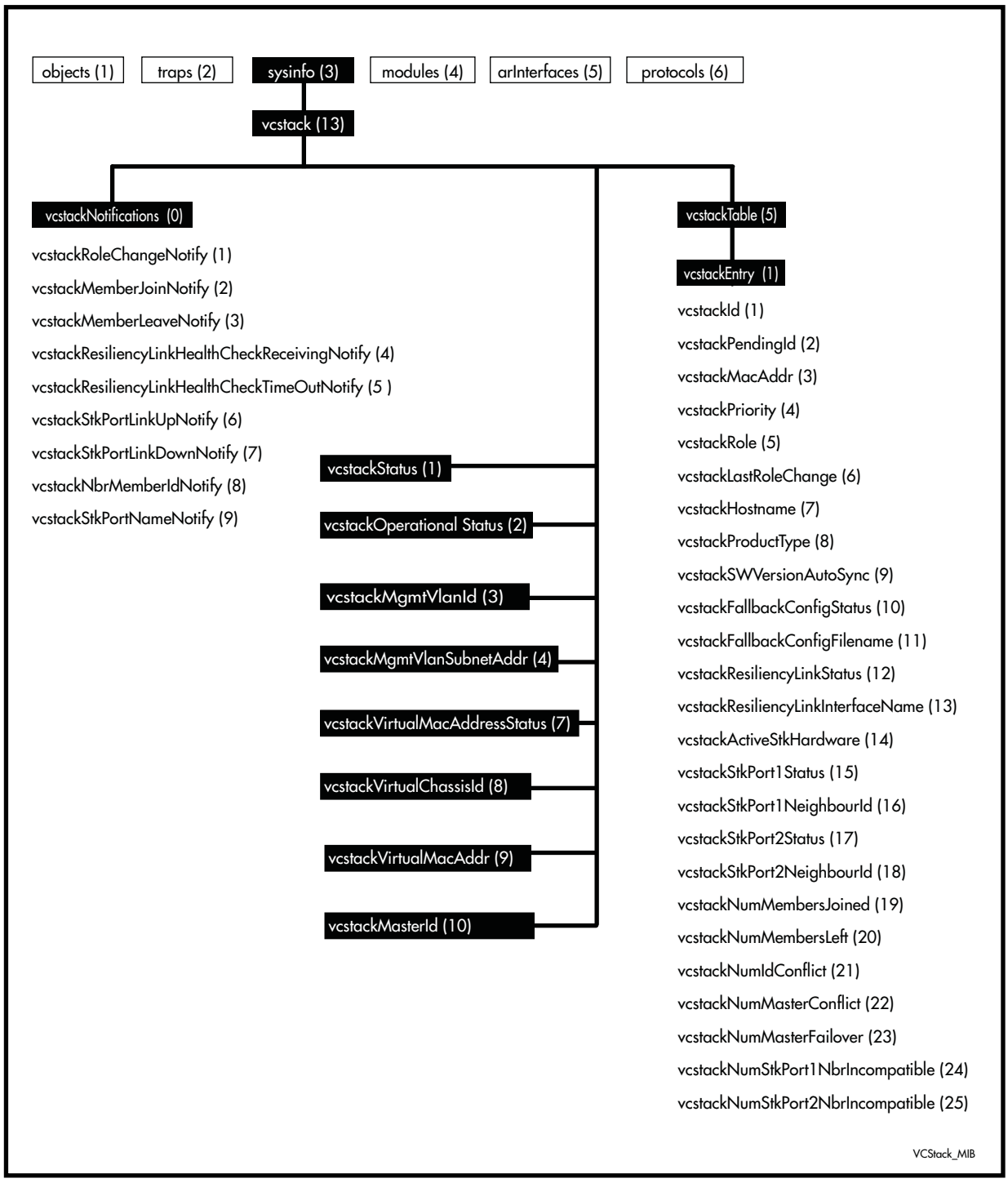


Table 68-25: Objects defined in AT-VCSTACK-MIB

Object	Object Identifier	Description
vcstack	{ sysinfo (13) }	Overall stack status.
vcstackNotifications	{ vcstack 0 }	List of traps (notifications) generated for the stack:
vcstackRoleChangeNotify	{ vcstackNotifications 1 }	The stack status can take one of the following states: 1. normalOperation (1) 2. operatingInFailoverState (2) 3. standaloneUnit (3) 4. ringTopologyBroken (4)
vcstackMemberJoinNotify	{ vcstackNotifications 2 }	Notification generated when a member joins the stack. Displays the objects: 1. vcstackId 2. vcstackNbrMemberId
vcstackMemberLeaveNotify	{ vcstackNotifications 3 }	Notification generated when a member leaves the stack. Displays the objects: 1. vcstackId 2. vcstackNbrMemberId
vcstackResiliencyLinkHealthCheckReceivingNotify	{ vcstackNotifications 4 }	Notification generated when the resiliency link is activated. Displays the objects: 1. vcstackId 2. vcstackResiliencyLinkInterfaceName
vcstackResiliencyLinkHealthCheckTimeOutNotify	{ vcstackNotifications 5 }	Notification generated when the backup member's receive timer has timed-out, indicating that the Backup has lost contact with the Master via the resiliency link. Displays the objects: 1. vcstackId 2. vcstackResiliencyLinkInterfaceName
vcstackStkPortLinkUpNotify	{ vcstackNotifications 6 }	Notification generated when the stack port link is up. Displays the objects: 1. vctasckId 2. vcstackStkPortName
vcstackStkPortLinkDownNotify	{ vcstackNotifications 7 }	Notification generated when the stack port link is down. Displays the objects: 1. vcstackId 2. vcstackStkPortName
vvcstackNbrMemberIdNotify	{ vcstackNotifications 8 }	The stack member id related to this trap
vcstackStkPortNameNotify	{ vcstackNotifications 9 }	The stack port name related to this trap

Table 68-25: Objects defined in AT-VCSTACK-MIB(cont.)

Object	Object Identifier	Description
vcstackOperationalStatus	{ vcstack 2 }	The operational status of the stack can be either: 1. enabled (1) 2. disabled (2)
vcstackMgmtVlanId	{ vcstack 3 }	The current stacking management VLAN ID
vcstackMgmtVlanSubnetAddr	{ vcstack 4 }	The current stacking management VLAN subnet address
vcstackTable	{ vcstack 5 }	Table of information about stack members, indexed by vcstackId.
vcstackEntry	{ vcstackTable 1 }	Information about a single stack member, indexed by vcstackId.
vcstackId	{ vcstackEntry 1 }	Stack member ID.
vcstackPendingId	{ vcstackEntry 2 }	Pending stack member ID.
vcstackMacAddr	{ vcstackEntry 3 }	Stack member's hardware MAC address.
vcstackPriority	{ vcstackEntry 4 }	Priority for election of the stack master. The lowest number has the highest priority.
vcstackRole	{ vcstackEntry 5 }	Stack member's role in the stack. Can be one of the following: 1. leaving (1) 2. discovering (2) 3. synchronizing (3) 4. backupMember (4) 5. pendingMaster (5) 6. disabledMaster (6) 7. fallbackMaster (7) 8. activeMaster (8)
vcstackLastRoleChange	{ vcstackEntry 6 }	Time and date when the stack member last changed its role in the stack.
vcstackHostname	{ vcstackEntry 7 }	Stack member's hostname.
vcstackProductType	{ vcstackEntry 8 }	Stack members product type.
vcstackSWVersionAutoSync	{ vcstackEntry 9 }	Whether or not the stack member's software is automatically upgraded.
vcstackFallbackConfigStatus	{ vcstackEntry 10 }	Status of the fallback configuration file. Can be one of: 1. fileExists (1) 2. fileNotFound (2) 3. notConfigured (3)

Table 68-25: Objects defined in AT-VCSTACK-MIB(cont.)

Object	Object Identifier	Description
vcstackFallbackConfigFilename	{ vcstackEntry 11 }	Filename of the fallback configuration file.
vcstackResiliencyLinkStatus	{ vcstackEntry 12 }	Status of the stack members resiliency link. Can be one of: 1. configured (1) 2. successful (2) 3. failed (3) 4. notConfigured (4)
vcstackResiliencyLinkInterfaceName	{ vcstackEntry 13 }	Name of the interface the resiliency link is configured on.
vcstackActiveStkHardware	{ vcstackEntry 14 }	Stack ports hardware type. Can be one of: 1. value (0) is now obsolete 2. xemStk (1) 3. builtinStackingPorts (2) 4. none (3) is now obsolete 5. stackXG (4)
vcstackStkPort1Status	{ vcstackEntry 15 }	Status of stack-port 1. Can be one of the following: 1. down (1) 2. neighbourIncompatible (2) 3. discoveringNeighbour (3) 4. learnedNeighbour (4)
vcstackStkPort1NeighbourId	{ vcstackEntry 16 }	ID of the neighbor on stack-port 1. Zero indicates no learned neighbor.
vcstackStkPort2Status	{ vcstackEntry 17 }	Status of stack-port 2. Can be one of: 1. down (1) 2. neighbourIncompatible (2) 3. discoveringNeighbour (3) 4. learnedNeighbour (4)
vcstackStkPort2NeighbourId	{ vcstackEntry 18 }	ID of the neighbor on stack-port 2. Zero indicates no learned neighbor.
vcstackNumMembersJoined	{ vcstackEntry 19 }	Number of times the stack has acquired a member.
vcstackNumMembersLeft	{ vcstackEntry 20 }	Number of times the stack has lost a member.
vcstackNumIdConflict	{ vcstackEntry 21 }	Number of times that a stack member ID conflict has occurred.
vcstackNumMasterConflict	{ vcstackEntry 22 }	Number of times that a stack master conflict has occurred.
vcstackNumMasterFailover	{ vcstackEntry 23 }	Number of times that the stack master has failed.

Table 68-25: Objects defined in AT-VCSTACK-MIB(cont.)

Object	Object Identifier	Description
vcstackNumStkPort1NbrIncompatible	{ vcstackEntry 24 }	Number of times that the neighbor on stack port 1 was incompatible.
vcstackNumStkPort2NbrIncompatible	{ vcstackEntry 25 }	Number of times that the neighbor on stack port 2 was incompatible.
vcstackVirtualMacAddressStatus	{vcstack 7}	Indicates whether the virtual MAC address is enabled or disabled. Read-only object.
vcstackVirtualChassisId	{vcstack 8}	Displays the current virtual chassis ID. Read-only object.
vcstackVirtualMacAddr	{vcstack 9}	Displays the virtual MAC address used by the stack. Read-only object.
vcstackMasterId	{vcstack 10}	Displays the stack ID of the master unit, or the stack ID of the standalone unit. Read-only object

Other Enterprise MIBs

In general, all objects are supported except where the relevant protocol or feature is either not supported or not applicable to the device. The following MIBs although under the Enterprise Branch (OID 1.3.6.1.4.1) and utilized by AlliedWare Plus products are not within the AlliedTelesis branch of the MIB object tree.

Public MIBs

The following table lists the public MIBs supported by the AlliedWare Plus™ Operating System. In general, all objects are supported except where the relevant protocol or feature is either not supported or not applicable to the device. Any variations from the standard are listed.

Public MIBs Supported by AlliedWare Plus™

MIB Name	Reference / Implementation
IANAifType-MIB	**www.iana.org/assignments/ianaiftype-mib**, IANAifType textual convention.
RFC1155-SMI	RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets.*
-	RFC 1212, *Concise MIB Definitions*.
RFC1213-MIB	See IP-MIB.
-	RFC 1215, *A Convention for Defining Traps for use with the SNMP*.
-	RFC 1239, *Reassignment of Experimental MIBs to Standard MIBs*.
IP-MIB	The IP MIB tree encompasses IP-MIB, RFC1213-MIB and IP-FORWARD-MIB definitions. The following documents define the components: ■ RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II* ■ RFC 4292, *IP Forwarding Table MIB* ■ RFC 4293, *Management Information Base for the Internet Protocol (IP)* The following objects **are** supported: ■ ipForwarding ■ ipDefaultTTL ■ All ipAddrTable objects except ipAdEntReasmMaxSize ■ All ipNetToPhysicalTable objects except ipNetToPhysicalRowStatus (all read-only) ■ ipCidrRouteNumber ■ All ipCidrRouteTable objects except ipCidrRouteTos All other objects in these MIBs are not supported. Note that an Enterprise version of ipAddressTable objects is provided by atIpAddressTable in AT-IP-MIB. This provides equivalent functionality along with support for primary and secondary IP addresses.
TCP-MIB	RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2*.
UDP-MIB	RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*.
IP-FORWARD-MIB	See IP-MIB.
-	RFC 2257, *Agent Extensibility (AgentX) Protocol Version 1*.
SNMP-MPD-MIB	RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.
SNMP-COMMUNITY-MIB	RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.
SNMPv2-SMI	RFC 2578, *Structure of Management Information Version 2 (SMIv2)*.
SNMPv2-TC	RFC 2579, *Textual Conventions for SMIv2*.

Public MIBs Supported by AlliedWare Plus™(cont.)

MIB Name	Reference / Implementation
SNMPv2-CONF	RFC 2580, *Conformance Statements for SMIv2*.
P-BRIDGE-MIB	RFC 2674, *Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*. The following objects are not supported: ■ dot1dTpPortOverflowTable ■ dot1dTrafficClassesEnabled ■ dot1dGmrpStatus ■ dot1dPortCapabilitiesTable ■ dot1dUserPriority ■ dot1dTrafficClassPriority ■ dot1dPortOutboundAccessPriorityTable ■ all objects in the dot1dGarp group ■ all objects in the dot1dGmrp group The following read-write object is implemented as read-only: ■ dot1dPortNumTrafficClasses
Q-BRIDGE-MIB	RFC 2674, *Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*. The following objects are not supported: ■ dot1qGvrpStatus ■ dot1qFdbId ■ dot1qTpFdbAddress ■ dot1qTpGroupTable ■ dot1qForwardAllTable ■ dot1qForwardUnregisteredTable ■ all objects in the dot1qStatic group ■ dot1qVlanTimeMark ■ dot1qVlanIndex ■ dot1qVlanCurrentEgressPorts ■ dot1qVlanCurrentUntaggedPorts ■ dot1qVlanForbiddenEgressPorts ■ dot1qPortGvrpStatus ■ dot1qPortGvrpFailedRegistrations ■ dot1qPortGvrpLastPduOrigin ■ dot1qPortRestrictedVlanRegistration ■ dot1qPortVlanStatisticsTable ■ dot1qPortVlanHCStatisticsTable ■ dot1qLearningConstraintsTable The following read-write objects are implemented as read-only: ■ dot1qPvid ■ dot1qPortAcceptableFrameTypes
HOST-RESOURCES-MIB	RFC 2790, *Host Resources MIB*. The following objects are not supported: ■ hrStorageAllocationFailures ■ All objects in hrDevice ■ All objects in hrSWRun ■ All objects in hrSWRunPerf ■ All objects in hrSWInstalled ■ All objects in hrMIBAdminInfo
SNMPv2-PDU	RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

Public MIBs Supported by AlliedWare Plus™ (cont.)

MIB Name	Reference / Implementation
SNMPv2-TM	RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*.
SNMPv2-MIB	RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.
POE-MIB	RFC 3621, Power Ethernet MIB. In each of the following objects, if one entry is set then all other entries for the same object in the table are set to the same value. ■ pethMainPseUsageThreshold ■ pethNotificationControlEnable The following objects indicate PSE threshold usage notification: ■ pethMainPowerUsageOnNotification ■ pethMainPowerUsageOffNotification The following read-write object is implemented as read-only: ■ pethPsePortPowerPairs
EtherLike-MIB	RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*. The following objects are deprecated: ■ dot3StatsEtherChipSet ■ all objects in the dot3Tests group ■ all objects in the dot3Errors group The following read-write object is implemented as read-only: ■ dot3PauseAdminMode
MAU-MIB	RFC 3636, *Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)*. The following objects are not supported: ■ all objects in the dot3RpMauBasicGroup group ■ ifMauTypeListBits ■ ifMauHCFalseCarriers ■ all object identifiers in the dot3MauType group ■ ifMauAutoNegCapabilityBits ■ ifMauAutoNegCapAdvertisedBits ■ ifMauAutoNegCapReceivedBits ■ ifMauAutoNegRemoteFaultAdvertised ■ ifMauAutoNegRemoteFaultReceived ■ all objects in the mauMod group The following objects are deprecated: ■ ifMauTypeList ■ all objects in the dot3BroadMauBasicGroup group ■ ifMauAutoNegCapability ■ ifMauAutoNegCapAdvertised ■ ifMauAutoNegCapReceived The following read-write object is implemented as read-only: ■ ifMauStatus
INET-ADDRESS-MIB	RFC 4001, *Textual Conventions for Internet Network Addresses*.

Public MIBs Supported by AlliedWare Plus™ (cont.)

MIB Name	Reference / Implementation
BRIDGE-MIB	RFC 4188, *Definitions of Managed Objects for Bridges*. The following read-write objects are implemented as read-only: ■ dot1dStpPortEnable ■ dot1dStpPortPathCost The following objects are not supported: ■ dot1dStaticTable ■ dot1dBaseDelayExceededDiscards ■ dot1dBasePortMtuExceededDiscards
RSTP-MIB	RFC 4318, *Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol.* The following read-write objects are implemented as read-only: ■ dot1dStpPortProtocolMigration ■ dot1dStpPortAdminEdgePort ■ dot1dStpPortAdminPointToPoint ■ dot1dStpPortAdminPathCost The following object is deprecated: ■ dot1dStpPathCostDefault
DISMAN-PING-MIB	RFC 4560, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*. The following (lldpLocManAddrTable and lldpConfigManAddrTable) read-write object is implemented as read-only: ■ pingMaxConcurrentRequests You can specify multiple ping operations, but the device only performs one ping at a time (pingMaxConcurrentRequests). The device uses ICMP echo for ping operations (pingImplementationTypeDomains).
LLDP-MIB	*IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions*. The following local management address table supports only a single management address per port: ■ lldpConfigManAddrTable
LLDP-EXT-DOT1-MIB	*IEEE Standard 802.1AB-2005, Annex F, IEEE 802.1 Organizationally Specific TLVs., Section F.7.1, IEEE 802.1LLDP extension MIB module*. In each of the following tables, if one entry is set, all other entries in the table are set to the same value. ■ lldpXdot1ConfigVlanNameTxEnable ■ lldpXdot1ConfigProtoVlanTxEnable ■ lldpXdot1ConfigProtocolTxEnable
LLDP-EXT-DOT3-MIB	*IEEE Standard 802.1AB-2005, Annex G, IEEE 802.3 Organizationally Specific TLVs, Section G.7.1, IEEE 802.3 LLDP extension MIB module*
LLDP-EXT-MED-MIB	*ANSI/TIA-1057- 2006, Section 13.3, LLDP-MED MIB Definition*
RIPv2-MIB	RFC1724 - RIP Version 2 MIB Extension

In general, all objects are supported except where the relevant protocol or feature is either not supported or not applicable to the device. The following table lists the private MIBs supported by the AlliedWare Plus™ Operating System. Any variations from the standard are listed.

Chapter 69: LLDP, LLDP-MED and Voice VLAN Introduction and Configuration

Introduction 69.2
Link Layer Discovery Protocol 69.2
LLDP-MED 69.3
Voice VLAN 69.3
LLDP Advertisements 69.4
  Type-Length-Value (TLV) 69.4
  LLDP-MED: Location Identification TLV 69.7
Transmission and Reception 69.8
  LLDP-MED Operation 69.9
Storing LLDP Information 69.10
Configuring LLDP 69.11
  Configure LLDP 69.12
  Configure LLDP-MED 69.14
  Configure Authentication for Voice VLAN 69.18

Introduction

This chapter describes the Link Layer Discovery Protocol (LLDP), LLDP for Media Endpoint Devices (LLDP-MED) and Voice VLAN, and general configuration information for these.

LLDP is designed to be managed with the Simple Network Management Protocol (SNMP), and SNMP-based Network Management Systems (NMS). LLDP can be configured, and the information it provides can be accessed, using either the command line interface or SNMP.

- For detailed descriptions of the commands used to configure LLDP and LLDP-MED, see **Chapter 70, LLDP Commands**.
- For Voice VLAN commands, see **Chapter 17, VLAN Commands**.
- For information about the LLDP and LLDP-MED MIBs, see **"Public MIBs" on page 68.83**.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol defined by the *IEEE Standard 802.1AB-2005*. This switch supports LLDP as specified in this standard, including *Annex F* and *Annex G*.

LLDP enables Ethernet network devices, such as switches and routers, to transmit and/or receive device-related information to or from directly connected devices on the network, and to store such information learned about other devices. The data sent and received by LLDP is useful for many reasons. The switch can discover neighbors—other devices directly connected to it. Devices can use LLDP to advertise some parts of their Layer 2 configuration to their neighbors, enabling some kinds of misconfiguration to be more easily detected and corrected.

LLDP is a link level ("one hop") protocol; LLDP information can only be sent to and received from devices that are directly connected to each other, or connected via a hub or repeater. Advertised information is not forwarded on to other devices on the network.

The information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgment.

LLDP operates over physical ports (Layer 2) only. For example, it can be configured on switch ports that belong to static or dynamic aggregated links (channel groups), but not on the aggregated links themselves; and on switch ports that belong to VLANs, but not on the VLANs themselves.

LLDP provides a way for the switch to:

- transmit information about itself to neighbors
- receive device information from neighbors
- store and manage information in an LLDP MIB

Each port can be configured to transmit local information, receive neighbor information, or both.

LLDP defines:

- a set of common advertisements (**"LLDP Advertisements" on page 69.4**)
- a protocol for transmitting and receiving advertisements (**"Transmission and Reception" on page 69.8**)
- a method for storing the information that is contained within received advertisements (**"Storing LLDP Information" on page 69.10**)

Interactions

LLDP has the following interactions with other switch features:

- Spanning tree

  Ports blocked by a spanning tree protocol can still transmit and receive LLDP advertisements.

- 802.1x

  Ports blocked by 802.1x port authorization cannot transmit or receive LLDP advertisements. If LLDP has stored information for a neighbor on the port before it was blocked, this information will eventually time out and be discarded.

- VLAN tagging

  LLDP packets are untagged; they do not contain 802.1Q header information with VLAN identifier and priority tagging.

- Virtual Chassis Stacking (VCStack) resiliency link

  When a port is configured as a VCStack resiliency link port, LLDP does not operate on the port; LLDP neither transmits nor receives advertisements, and any LLDP configuration and data stored for the port, including counters, is discarded.

- Mirror ports

  LLDP does not operate on mirror analyzer ports.

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED), is an extension of LLDP used between LAN network connectivity devices, such as this switch, and the media endpoint devices connected to them, such as IP phones. LLDP-MED is specified in *ANSI/TIA-1057-2006*. Of the application types specified in *ANSI/TIA-1057-2006*, the switch supports Application Type 1: Voice.

LLDP-MED uses the LLDP advertisement, transmission and storage mechanisms, but transmits, receives, and stores data specifically related to managing the voice endpoint devices. This includes information about network policy, location, hardware configuration, and, for Power over Ethernet-capable devices, power management.

Voice VLAN

Many IP phones (or other IP voice devices) have two interfaces: one to connect to the network and another that allows a computer or similar device to connect to the network via the IP phone. It is often desirable to treat the voice and data traffic separately so that appropriate Quality of Service (QoS) policies can be applied to each. The Voice VLAN feature uses LLDP-MED to convey configuration information (such as VLAN ID and User Priority tagging, and DiffServ Code Point (DSCP)—**"Differentiated Services Architecture" on page 40.4**) for the voice traffic to the IP phone. In response, the IP

phone sends voice traffic according to this configuration. The data traffic coming through the IP phone from the PC is sent with the default configuration, typically untagged with normal priority.

LLDP Advertisements

LLDP transmits advertisements as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

Type-Length-Value (TLV)

A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data, such as variable length strings, in a standardized format. Each TLV advertises a single type of information, such as its device ID, type, or management addresses. The following table describes fields in a TLV.

Table 69-1: Fields in a Type Length Value element

Field	Description
Type	Identifies the kind of information. It consists of a 7-bit Type code.
Length	Identifies the length of the information. It consists of a 9-bit value that specifies the number of bytes of data in the Value field.
Value	Contains the actual value of the advertised information. This is a variable length data field.

LLDP sends mandatory TLVs in each advertisement; it can also be configured to send one or more optional TLVs, from the following groups:

- Mandatory Base TLVs, included in all LLDP advertisements. See IEEE 802.1AB-2005.
- Optional Base TLVs, which may be included in any LLDP advertisements. See IEEE 802.1AB-2005.
- IEEE 802.1 Organizationally Specific TLVs (802.1 TLVs). See IEEE 802.1AB-2005 Annex F.
- IEEE 802.3 Organizationally Specific TLVs (802.3 TLVs). See IEEE 802.1AB-2005 Annex G.
- LLDP-MED Organizationally Specific TLVs (LLDP-MED TLVs), included in LLDP-MED advertisements. See ANSI/TIA-1057- 2006.

Mandatory and optional TLVs for LLDP and LLDP-MED advertisements are shown in **Table 69-2**.

Table 69-2: TLVs in LLDP advertisements

TLV	Description
Mandatory Base TLVs—IEEE 802.1AB-2005	
Chassis ID	Identifies the device's chassis. On this switch, this is the MAC address of the switch or stack.
Port ID	Identifies the port that transmitted the LLDPDU.

Table 69-2: TLVs in LLDP advertisements(cont.)

TLV	Description
Time To Live (TTL)	Indicates the length of time in seconds for which the information received in the LLDPDU remains valid. If the value is greater than zero, the information is stored in the LLDP remote system MIB. If the value is zero, the information previously received is no longer valid, and is removed from the MIB.
End of LLDPDU	Signals that there are no more TLVs in the LLDPDU.
Optional Base TLVs—IEEE 802.1AB-2005	
Port description	A description of the device's port in alpha-numeric format.
System name	The system's assigned name in alpha-numeric format.
System description	A description of the device in alpha-numeric format. This includes information about the device's hardware and operating system.
System capabilities	The device's router and bridge functions, and whether or not these functions are currently enabled.
Management address	The address of the local LLDP agent. This can be used to obtain information related to the local device.
IEEE 802.1 Organizationally Specific TLVs (802.1 TLVs)—IEEE 802.1AB-2005 Annex F	
Port VLAN	VLAN identifier that the local port associates with untagged or priority tagged frames.
Port & Protocol VLANs	Whether Port & Protocol VLAN is supported and enabled on the port, and the list of Port & Protocol VLAN identifiers.
VLAN Names	List of VLAN names that the port is assigned to.
Protocol IDs	List of protocols that are accessible through the port, for instance: ■ 9000 (Loopback) ■ 00 26 42 42 03 00 00 00 (STP) ■ 00 27 42 42 03 00 00 02 (RSTP) ■ 00 69 42 42 03 00 00 03 (MSTP) ■ 888e01 (802.1x) ■ aa aa 03 00 e0 2b 00 bb (EPSR) ■ 88090101 (LACP) ■ 00540000e302 (Loop protection) ■ 0800 (IPv4) ■ 0806 (ARP) ■ 86dd (IPv6)

Table 69-2: TLVs in LLDP advertisements(cont.)

TLV	Description
IEEE 802.3 Organizationally Specific TLVs (802.3 TLVs)—IEEE 802.1AB-2005 Annex G	
MAC/PHY Configuration/ Status	The current values of the following for the port: ■ Speed and duplex mode auto-negotiation support ■ Auto-negotiation status ■ PMD (physical media dependent) auto-negotiation advertised capability ■ Operational MAU type This TLV is always included in LLDP-MED advertisements.
Power Via MDI	The power-via-MDI capabilities. On devices that are LLDP-MED and PoE-capable, we recommend using the Extended Power-via-MDI TLV instead of this TLV.
Link Aggregation	Whether the link is capable of being aggregated, whether it is currently in an aggregation and if in an aggregation, the port of the aggregation.
Maximum Frame Size	The maximum supported 802.3 frame size that the sending device is capable of receiving—larger frames will be dropped.
LLDP-MED Organizationally Specific TLVs (LLDP-MED TLVs)—ANSI/TIA-1057- 2006	
LLDP-MED Capabilities	Indicates an LLDP-MED capable device, and advertises which LLDP-MED TLVs are supported and enabled, and the device type. For this switch, the device type is Network Connectivity Device. An advertisement containing this TLV is an LLDP-MED advertisement.
Network Policy	Network policy information configured on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data: ■ Voice VLAN ID ■ Voice VLAN User Priority tagging ■ Voice VLAN Diffserv Code Point (DSCP)
Location Identification	Location information configured for the port, in one or more of the following formats: ■ Civic address ■ Coordinate-based LCI ■ Emergency Location Identification Number (ELIN) For more information, see **"LLDP-MED: Location Identification TLV" on page 69.7**.
Extended Power-via-MDI	For PoE-capable devices, this TLV includes: ■ Power Type field: Power Sourcing Entity (PSE). ■ Power Source field: current power source, either Primary Power Source or Backup Power Source. ■ Power Priority field: power priority configured on the port. ■ Power Value field: In TLVs transmitted by Power Sourcing Equipment (PSE) such as this switch, this advertises the power that the port can supply over a maximum length cable based on its current configuration (that is, it takes into account power losses over the cable). In TLVs received from Powered Device (PD) neighbors, the power value is the power the neighbor requests. Available on devices that are PoE-capable.

Table 69-2: TLVs in LLDP advertisements(cont.)

TLV	Description
Inventory Management TLV Set	Includes the following TLVs, based on the current hardware platform and the software version, identical on every port on the switch: ■ Hardware Revision ■ Firmware Revision ■ Software Revision ■ Serial Number ■ Manufacturer Name ■ Model Name ■ Asset ID On Virtual Chassis Stacking devices, the inventory information is based on the current master.

LLDP-MED: Location Identification TLV

Location information can be configured for each port, and advertised to remote devices, which can then transmit this information in calls; the location associated with voice devices is particularly important for emergency call services. All ports may be configured with the location of the switch, or each port may be configured with the location of the remote voice device connected to it.

The location information for a particular port can be configured using one or more of the following three data formats: coordinate-based, Emergency Location Identification Number (ELIN), and civic address. Up to one location of each type can be assigned to a port.

Location configuration information (LCI) in all configured data formats is transmitted in Location Identification TLVs. When LLDP receives a Location Identification TLV, it updates the remote entry in the LLDP-MED MIB with this information.

Co-ordinate LCI Coordinate-based location data format uses geospatial data, that is, latitude, longitude, and altitude (height or floors), including indications of resolution, with reference to a particular datum: WGS 84, NAD83—North American Vertical Datum of 1988 (NAVD88), or NAD83—Mean Lower Low Water (MLLW). For more information, see *RFC 3825, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*.

ELIN LCI Emergency Location Identification Number (ELIN) location data format provides a unique number for each location for Emergency Call Services (ECS). In North America, ELINs are typically 10 digits long; ELINs up to 25 digits are supported.

Civic Address LCI The Civic Address location data format uses common street address format, as described in *RFC4776*.

Transmission and Reception

Table 69-3 describes the LLDP transmission and reception processes. Additional LLDP-MED processes are described in **"LLDP-MED Operation" on page 69.9**.

Table 69-3: LLDP transmission and reception processes

When ...	and ...	then ...
LLDP is enabled	Ports are configured to transmit LLDP advertisements	Regular LLDP advertisements are sent via these ports at intervals determined by the transmit interval. Each advertisement contains local information (from the Local Systems MIB) for all the mandatory TLVs and the optional TLVs that the port is configured to send.
	Ports are configured to receive LLDP advertisements	Information received in advertisements via these ports is stored in the Neighbor table (Remote Systems MIB). This information is retained until it is replaced by a more recent advertisement from the same neighbor or it times out (the TTL elapses).
Local information changes	The transmission delay time has elapsed since the last advertisement was transmitted	New advertisements are sent containing the new set of local information.
Neighbor information changes	Notifications are enabled, and the notification interval has elapsed since the last notification was sent	The SNMP notification (trap) lldpRemTablesChange is sent.
LLDP transmission and reception is disabled on a port.	An LLDP command was used to do this	It transmits a final 'shutdown' LLDPDU with a Time-To-Live (TTL) TLV that has a value of "0". This tells any remote neighboring devices to remove the information associated with this switch from their remote systems MIB. Then it stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	A shutdown command was used on the port	It makes a best effort to send a shutdown LLDPDU. Then it stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	Something else disabled LLDP, such as Virtual Chassis Stacking (VCStack) failover	It does not send a shutdown LLDPDU. It stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	It is enabled again	LLDP reinitializes and resumes transmitting and receiving advertisements after the reinitialization interval has elapsed.
The Neighbor table has 1600 neighbors		It discards any further neighbors.
LLDP receives a LLDPDU or TLV with a detectable error		It discards the incorrect TLV.
LLDP receives a TLV it does not recognize	It contains no basic format errors	It stores it for possible later retrieval by network management (in the unrecognized TLV information table lldpRemUnknownTLVTable in the LLDP MIB).

LLDP-MED Operation

When LLDP is enabled, LLDP-MED is enabled by default, and uses the same LLDP transmission and reception process described in **Table 69-3**. When LLDP receives an advertisement indicating a newly connected LLDP-MED-capable device on a port, it transmits one LLDP-MED advertisement per second via this port, a configurable number of times (the *fast start count*). Thereafter, it sends regular advertisements at the LLDP transmit interval. When the last advertisement for an LLDP-MED-capable device connected to the port times out, it stops sending LLDP-MED advertisements via the port.

If LLDP-MED notifications are enabled for a port, and SNMP traps for LLDP are enabled, LLDP-MED generates a *Topology Change Notification (LLDP-MED lldpXMedTopology ChangeDetected)* when a new LLDP-MED compliant IP telephony device is connected to a port or removed from a port. This notification includes the following information:

- IP Phone Chassis ID and Chassis ID sub-type (IP address)
- LLDP Endpoint Device Class
- Switch Chassis ID (MAC address) and Port ID where the device is attached.

Storing LLDP Information

When an LLDP device receives a valid LLDP advertisement from a neighboring network device, it stores the information in an IEEE-defined Simple Network Management Protocol (SNMP) Management Information Base (MIB).

LLDP stores information in the LLDP MIB defined in Section 12 of the *IEEE Standard 802.1AB-2005*, its extensions defined in *Annex F*, *Annex G*, and ANSI/TIA-1057- 2006, about:

LLDP-EXT-MED-MIB ANSI/TIA-1057- 2006, Section 13.3, LLDP-MED MIB Definition

- Local system information. This is the information that LLDP can transmit in advertisements to its neighbors.
- Remote systems information. This is the data that the device receives in advertisements from its neighbors.
- LLDP configuration. This can be used with SNMP to configure LLDP on the device.
- LLDP statistics. This includes information about LLDP operation on the device, including packet and event counters.

This information can be accessed either via SNMP, or directly using the command line interface.

Local system

Information about your device is called local system information. The LLDP local system MIB maintains this information, which consists of device details, as well as any user-configured information that you have set up for your switch, for example a port description or a management address.

LLDP on this device can store one management address per port, and transmit this in LLDP advertisements. It can store multiple management addresses received from each neighbor.

Remote systems

Information gained from neighboring devices is called remote system information. The LLDP remote systems MIB maintains this information.

The length of time for which neighbor information remains in the LLDP remote systems MIB is determined by the Time-To-Live (TTL) value of received LLDPDUs. When it receives an advertisement from a neighbor, LLDP starts a timer based on the Time To Live (TTL) information in the advertisement. The Time To Live (TTL) information in an advertisement is:
TTL=transmit interval x holdtime multiplier. If the TTL elapses, for instance if the neighbor has been removed, LLDP deletes the neighbor's information from the MIB. This ensures that only valid LLDP information is stored.

Whenever a new neighbor is discovered, or an existing neighbor sends an advertisement with new information that differs from the previous advertisement, for example a new or changed TLV, a remote tables change event is activated. If SNMP notifications are enabled, the notification lldpRemTablesChange is sent.

To prevent the remote systems MIB from using large amounts of memory and possibly affecting the operation of your switch, it limits the number of neighbors it stores information for to 1600. If it is storing information from 1600 neighbors, and detects any more neighbors, it is considered to have too many neighbors, and discards advertisements from the rest. There is no per-port limit to the number of neighbors.

SNMP utilities

An SNMP utility can read the Neighbors table MIB (Remote Systems Data in the LLDP MIB) on a device to find out about the LLDP neighbors it is directly connected to on each port. Then it can read the Neighbors table MIB on each of these neighbors to find out about their neighboring LLDP devices, and so on.

Configuring LLDP

You can configure LLDP on the device using either:

- the command line interface. For detailed descriptions of the commands, see **Chapter 70, LLDP Commands**, or
- SNMP—see **Chapter 68, SNMP MIBs**.

This section includes the following command line interface configuration procedures:

- **"Configure LLDP" on page 69.12**— This procedure includes configuration for LLDP between network connectivity devices; it does not include LLDP-MED. If you are configuring LLDP-MED only, use the following procedure instead of this one.
- **"Configure LLDP-MED" on page 69.14**—This procedure includes the LLDP configuration required to support LLDP-MED, as well as specific LLDP-MED and Voice VLAN configuration.
- **"Configure Authentication for Voice VLAN" on page 69.18**—This procedure includes 802.1X port authentication configuration including dynamic VLAN assignment to be used with LLDP-MED. Use the previous procedure before using this one.

Because LLDP is often used together with SNMP, consider configuring SNMP before you configure LLDP. LLDP transmits large amounts of data about the network. For security reasons, we recommend configuring SNMP for SNMP version 3 only (for read and write access). Remove all SNMPv1 and SNMPv2 configuration. See **Chapter 66, SNMP Introduction**, and **Chapter 67, SNMP Commands**.

Configure LLDP

Use the procedure in **Table 69-4** below to configure LLDP.

Some optional TLVs send information that can be configured by other commands. If LLDP will be configured to send these TLVs, consider whether to configure the corresponding parameters first.

- Port Description. See the **description (interface)** command on page 12.2.
- System Name. See the **hostname** command on page 8.17.

Table 69-4: Configuration procedure for LLDP

Step 1. Enable LLDP		
1.	`awplus#`**configure terminal**	Enter Configuration mode.
2.	`awplus(config)#`**lldp run**	Enable LLDP.
Step 2. Configure ports for LLDP Configure each port to determine whether and which LLDP messages are transmitted and received. If all the ports running LLDP require the same configuration, configure them all together. Otherwise repeat these commands for each port or group of ports that requires a particular configuration.		
3.	`awplus(config)# interface <port-list>`	Enter Interface Configuration mode for the switch ports.
4.	`awplus(config-if)#`**lldp tv-select {[<*tlv*>]...}** `awplus(config-if)#`**lldp tlv-select all**	By default, the mandatory TLVs are included in LLDP messages. Enable the transmission of one or more optional TLVs through these port as required.
5.	`awplus(config-if)#`**exit**	Return to Global Configuration mode.
6.	`awplus(config)#interface <port-list>`	By default, transmission and reception of LLDP advertisements is enabled on all ports. Enter Interface Configuration mode for any switch ports that should have transmission or reception disabled.
7.	`awplus(config-if)#`**no lldp {[transmit] [receive]}**	Disable transmission and/or reception as required.
8.	`awplus(config-if)#`**exit**	Return to Global Configuration mode.
9.	`awplus(config)#`**exit**	Return to Privileged Exec mode.
Step 3. Check LLDP configuration		
10.	`awplus#`**show lldp** `awplus#`**show lldp interface [<*port-list*>]** `awplus#`**show lldp local-info [base] [dot1] [dot3] [med] [interface <*port-list*>]** `awplus#`**show running-config lldp**	Review the LLDP configuration.
Step 4. Monitor LLDP		
11.	`awplus#`**show lldp neighbors** `awplus#`**show lldp neighbors detail** `awplus#`**show lldp statistics** `awplus#`**show lldp statistics interface [<*port-list*>]**	Monitor LLDP operations and display neighbor information as required.

Table 69-4: Configuration procedure for LLDP (cont.)

Step 5. Advanced LLDP configuration The configuration procedure above and the defaults for other settings suit most networks. Use the following commands for fine tuning if necessary. Timer intervals should be long enough not to create unnecessarily high numbers of advertisements when there are topology changes. However, be aware that if the intervals are long, a neighbor's information can continue to be stored after its information has changed, or after it is disconnected.		
12.	`awplus#`**configure terminal**	Enter Configuration mode.
13.	`awplus(config)#interface <port-list>`	Enter Interface Configuration mode for the switch ports.
14.	`awplus(config-if)#`**lldp management-address** ***<ipaddr>***	Override the default LLDP management address advertised through this port if required. This must be an IPv4 address that is already configured on the device. To see the management address that will be advertised, use the **show lldp local-info** command on page 70.39.
15.	`awplus(config-if)#`**lldp notifications**	By default, SNMP notifications are not transmitted. Enable them for these ports if required. (SNMP LLDP traps (notifications) must also be enabled.)
16.	`awplus(config-if)#`**exit**	Return to Global Configuration mode.
17.	`awplus(config)#`**lldp timer** ***<5-32768>***	The transmit interval determines how often regular LLDP transmits advertisements from each port. The transmit interval must be at least four times the transmission delay. Default: 30 seconds
18.	`awplus(config)#`**lldp notification-interval** ***<5-3600>***	The notification interval determines the minimum interval between sending SNMP notifications (traps). Default: 5 seconds
19.	`awplus(config)#`**lldp tx-delay** ***<1-8192>***	A series of successive changes over a short period of time can trigger the agent to send a large number of LLDPDUs. To prevent this, there is a transmission delay timer. This establishes a minimum length of time that must elapse between successive LLDP transmissions. The transmission delay cannot be greater than a quarter of the transmit interval. Default: **2** seconds
20.	`awplus(config)#`**lldp reinit** ***<1-10>***	Reinitialization delay timer determines the minimum time after disabling LLDP on a port before it can reinitialize. Default: **2** seconds
21.	`awplus(config)#`**lldp holdtime-multiplier** ***<2-10>***	The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors. Default: **4**
22.	`awplus(config)#`**exit**	Return to Privileged Exec mode.
Step 6. Clear data If necessary, you can clear either neighbor information or LLDP statistics for particular ports or all ports.		
23.	`awplus#`**clear lldp table [interface <port-list>]**	Clear the information from the table of neighbor information.
24.	`awplus#`**clear lldp statistics [interface** ***<port-list>*****]**	Clear LLDP statistics (packet and event counters).

Configure LLDP-MED

Use the procedure in **Table 69-5** to configure LLDP-MED and Voice VLAN for voice devices connected to the switch.

Consider whether you also need to configure:

- Simple Network Management Protocol (**Chapter 67, SNMP Commands**)
- 802.1X port authentication (**Chapter 47, 802.1X Commands**, **Chapter 43, Authentication Commands**, **Chapter 45, AAA Commands**)
- RADIUS server (**Chapter 49, RADIUS Commands**)
- Quality of Service (**Chapter 41, QoS Commands**)
- Access Control Lists (**Chapter 37, IPv4 Hardware Access Control List (ACL) Commands** and **Chapter 38, IPv4 Software Access Control List (ACL) Commands**)
- Power over Ethernet (PoE), if the switch supports PoE (**Chapter 23, Power over Ethernet Commands**)

In most cases, configuring LLDP-MED using SNMP or using the CLI command line interface (CLI) described in **Chapter 70, LLDP Commands** has the same effect. However, the effect of configuring location information using SNMP differs from the CLI. When location information is assigned to a port by SNMP and a matching location is not found on the device, then a new location is automatically created and assigned to the specified port. If the location is unset by SNMP later, then the location is removed to prevent accumulating SNMP-set location information. However, if the location is being used for other ports, the automatically created location is not removed until no ports use it. Once it is modified or assigned to other ports by CLI commands, the location remains even after no ports use the location.

Table 69-5: Configuration procedure for Voice VLAN and LLDP-MED

Step 1. Configure a Voice VLAN Create a VLAN for voice data from voice endpoint devices connected to ports on the switch. Specify the network policy for voice data in this voice VLAN. LLDP-MED sends the network policy to voice devices connected to these ports. The voice devices use this network policy to determine the VLAN, priority and DSCP tagging of voice data it transmits.		
1.	`awplus#` **configure terminal**	Enter Global Configuration mode.
2.	`awplus(config)#` **vlan database**	Enter VLAN Database Configuration mode.
3.	`awplus(config-vlan)#` **vlan** *<vid>* **[name** *<vlan-name>***] [state {enable|disable}]**	Create a VLAN to be used for the voice data to and from voice devices connected to the switch. By default, the new VLAN is enabled.
4.	`awplus(config-vlan)#` **exit**	Return to global configuration mode.
5.	`awplus(config)# interface` *<port-list>*	Enter interface configuration mode for the ports to be configured with the same network policy. This may be all the switch ports with voice devices connected to them, or a subset if the network policy will differ between ports.
6.	`awplus(config-if)#` **switchport voice vlan [***<vid>***|dot1p|dynamic|untagged]**	Specify the VLAN tagging to be used for voice data on these ports. Use the **dynamic** option if the VLAN tagging will be allocated dynamically by a RADIUS server. Default: **none**.
7.	`awplus(config-if)#` **switchport voice vlan priority** ***<0-7>***	Specify the priority-tagging that voice endpoint devices should put into their data packets. Default: **5**.

Table 69-5: Configuration procedure for Voice VLAN and LLDP-MED(cont.)

8.	`awplus(config-if)#` **switchport voice dscp** ***<0-63>***	Specify the DSCP value that voice endpoint devices should put into their data packets. Default: **0**.
9.	`awplus(config-if)#` **exit**	Return to global configuration mode.
Step 2. Enable LLDP		
10.	`awplus(config)#` **lldp run**	Enable LLDP on the switch. Default: LLDP is disabled.
11.	`awplus(config)# interface <port-list>`	Enter interface configuration mode for the switch ports LLDP is NOT to run on.
12.	`awplus(config-if)#` **no lldp {[transmit] [receive]}**	Disable transmission or reception on these ports as required. Default: **transmit** and **receive** enabled.
13.	`awplus(config-if)#` **exit**	Return to global configuration mode.
Step 3. Configure LLDP-MED location information Create civic address, coordinate, and/or ELIN locations, and assign them to switch ports.		
14.	`awplus(config)#` **location civic-location identifier** ***<civic-loc-id>***	Specify a civic location ID, and enter configuration mode for this identifier.
15.	`awplus(config-civic)#` **country** ***<country>*** `awplus(config-civic)#` **city** ***<city>*** `awplus(config-civic)#` **primary-road-name** ***<primary-road-name>*** `awplus(config-civic)#` **street-suffix** ***<street-suffix>*** `awplus(config-civic)#` **house-number** ***<house-number>*** `awplus(config-civic)#` *<other-civic-location-parameters …>*	Specify the civic address location information for the civic address location ID. You must specify a country first, using the upper-case two-letter country code, and then at least one more parameter. For the full set of parameters you can use to specify civic address location, see the **location civic-location configuration** command on page 70.22.
16.	`awplus(config-civic)#` **exit**	Return to global configuration mode.
17.	`awplus(config)#` **location coord-location identifier** ***<coord-loc-id>***	Specify a coordinate location identifier, and enter configuration mode for this identifier.
18.	`awplus(config-coord)#` **latitude** ***<latitude>*** `awplus(config-coord)#` **lat-resolution** ***<lat-resolution>*** `awplus(config-coord)#` **longitude** ***<longitude>*** `awplus(config-coord)#` **long-resolution** ***<long-resolution>*** `awplus(config-coord)#` **altitude** ***<altitude>*** **{meters|floor}** `awplus(config-coord)#` **alt-resolution** ***<alt-resolution>*** `awplus(config-coord)#` **datum {wgs84|nad83-navd|nad83-mllw}**	Specify the coordinate location for the coordinate location identifier.
19.	`awplus(config-coord)#` **exit**	Return to global configuration mode.
20.	`awplus(config)#` **location elin-location** ***<elin>*** **identifier** ***<elin-loc-id>***	Specify an ELIN location identifier, and the ELIN for this identifier.

Table 69-5: Configuration procedure for Voice VLAN and LLDP-MED(cont.)

21.	`awplus(config)# interface <port-list>`	Enter interface configuration mode for one or more switch ports which require the same location information.
22.	`awplus(config-if)#` **location civic-location-id <*civic-loc-id*>** `awplus(config-if)#` **location coord-location-id <*coord-loc-id*>** `awplus(config-if)#` **location elin-location-id <*elin-loc-id*>**	Assign the civic, coordinate, and/or ELIN location identifier to these ports. LLDP-MED will send the location information associated with a port to the voice endpoint device attached to it.
23.	`awplus(config-if)#` **exit**	Return to global configuration mode.
24.	`awplus(config)#` **exit**	Return to Privileged Exec mode.
Step 4. Review the LLDP configuration		
25.	`awplus#` **show lldp**	Check general LLDP configuration settings.
26.	`awplus#` **show lldp interface [<*port-list*>]**	Check LLDP configuration for ports.
27.	`awplus#` **show lldp local-info [base] [dot1] [dot3] [med] [interface <*port-list*>]**	Check the information that may be transmitted in LLDP advertisements from ports.
28.	`awplus#` **show location {civic-location|coord-location|elin-location}** `awplus#` **show location {civic-location|coord-location|elin-location} identifier {<*civic-loc-id*>|<*coord-loc-id*>|<*elin-loc-id*>}** `awplus#` **show location {civic-location|coord-location|elin-location} interface <*port-list*>**	Check the location information.
29.	`awplus#` **show running-config lldp**	If you want to display all the LLDP configuration, use this command.
Step 5. Monitor LLDP-MED		
30.	`awplus#` **show lldp neighbors [interface <*port-list*>]** `awplus#` **show lldp neighbors detail [base] [dot1] [dot3] [med] [interface <*port-list*>]** `awplus#` **show lldp statistics** `awplus#` **show lldp statistics interface [<*port-list*>]**	Monitor LLDP operation.
Step 6. Advanced configuration The configuration procedure above and the defaults for other settings suit most networks. Use the following commands for fine tuning if necessary. For information about other advanced configuration for LLDP, including LLDP timers, see **Table 69-4**.		
31.	`awplus#`**configure terminal**	Enter Global Configuration mode.
32.	`awplus(config)#` **lldp faststart-count <*1-10*>**	By default, when LLDP-MED detects an LLDP-MED capable device on a port, it sends 3 advertisements at 1s intervals. Change the fast start count if required. Default: fast start count is 3

Table 69-5: Configuration procedure for Voice VLAN and LLDP-MED(cont.)

33.	`awplus(config)#` **lldp non-strict-med-tlv-order-check**	By default non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, and LLDP-MED TLVs in non-standard order are discarded. If you require LLDP-MED advertisements with non-standard TLV order to be received and stored, enable non-strict order checking.
34.	`awplus(config)# interface <port-list>`	Enter interface configuration mode for switch ports which will have the same advanced configuration.
35.	`awplus(config-if)#` **lldp management-address <*ipaddr*>**	Override the default LLDP management address advertised through this port if required. This must be an IPv4 address that is already configured on the device. To see the management address that will be advertised, use the **show lldp local-info** command on page 70.39.
36.	`awplus(config-if)#` **lldp med-notifications**	By default, SNMP notifications are not transmitted. Enable LLDP-MED Topology Change Detected notifications for these ports if required. (SNMP LLDP traps (notifications) must also be enabled.) Default: LLDP-MED notifications disabled
37.	`awplus(config-if)#` **lldp tlv-select {[<*tlv*>]...}**	Enable the transmission of one or more optional LLDP TLVs in LLDP-MED advertisements through this port as required. The **mac-phy-config** TLV is transmitted in LLDP-MED advertisements whether or not it is enabled by this command. Default: all mandatory TLVs are enabled.
38.	`awplus(config-if)#` **lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}** `awplus(config-if)#` **lldp med-tlv-select all** `awplus(config-if)#` **no lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}** `awplus(config-if)#` **no lldp med-tlv-select all**	Enable or disable the transmission of optional LLDP-MED TLVs in LLDP-MED advertisements through these ports as required. Default: **capabilities**, **network-policy**, **location**, **power-management** are enabled.
39.	`awplus(config-if)#` **exit**	Return to global configuration mode.
40.	`awplus(config)#` **exit**	Return to privileged exec mode.
Step 7. Clear data If necessary, you can clear either neighbor information or LLDP statistics for particular ports or all ports.		
41.	`awplus#` **clear lldp table [interface <port-list>]**	Clear the information from the table of neighbor information.
42.	`awplus#` **clear lldp statistics [interface <*port-list*>]**	Clear LLDP statistics (packet and event counters).

Configure Authentication for Voice VLAN

Use the following procedure with LLDP-MED and Voice VLAN to configure 802.1X port authentication and dynamic VLAN assignment using a RADIUS server.

This procedure assumes that you have already:

- configured Voice VLAN and LLDP-MED using the procedure in **Table 69-5 on page 69.14**
- set **switchport voice vlan** to **dynamic** in the above procedure

Table 69-6: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN

Step 1.	**Configure the IP address of the RADIUS server.**	
1.	`awplus#`**configure terminal**	Enter Global Configuration mode.
2.	`awplus(config)#`**radius-server host** *<server-ip-address>* key *<key-string>*	Configure the IP address for the RADIUS server. Set the key that Network Access Servers (NAS) will need to use to get access to this RADIUS server. RADIUS server hosts configured using this command are included in the default RADIUS server group.
Step 2.	**Create VLANs.**	
3.	`awplus(config)#` **vlan database**	Enter VLAN Database Configuration mode.
4.	`awplus(config-vlan)#` **vlan** *<vid-range>*	Create the VLANs.
5.	`awplus(config-vlan)#` **exit**	Return to Global Configuration mode.
Step 3.	**Configure 802.1X port authentication.**	
6.	`awplus(config)#` **aaa authentication dot1x** default group radius	Enable 802.1X port authentication and set it to use the default group of RADIUS servers that contains all RADIUS server hosts configured using the **radius-server host** command.
7.	`awplus(config)# interface <port-list>`	Enter interface configuration mode for the ports that have users (PCs and phones) connected to them.
8.	`awplus(config-if)#` **dot1x port-control** auto	Enable 802.1X for port authentication on these ports.
9.	`awplus(config-if)#` **auth host-mode** multi-supplicant	Configure the ports to use multi-supplicant mode for authentication, so that the phone and PC can be dynamically allocated to different VLANs.
10.	`awplus(config-if)#` **auth dynamic-vlan-creation**	Configure the ports to accept dynamic VLAN allocation. In this procedure, the RADIUS server user groups for both the PCs and the phones use the same VLAN, so the default rule (**deny**) allows them both the access they need to the port VLAN. For other options, see the **auth dynamic-vlan-creation** command on page 43.6. Default: **deny** differently assigned VLAN IDs.
11.	`awplus(config-if)#` **exit**	Return to Global Configuration mode.

Table 69-6: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN(cont.)

12.	`awplus(config)#` **exit**	Return to Privileged Exec mode.
Step 4. Review the authentication configuration.		
13.	`awplus#` **show vlan {all|brief|dynamic|static|auto| static-ports<*1-4094*>}**	Check the VLAN configuration.
14.	`awplus#` **show dot1x [all]**	Check the 802.1X authentication configuration.

Chapter 70: LLDP Commands

Introduction 70.2
Command List 70.2
clear lldp statistics 70.2
clear lldp table 70.3
debug lldp 70.4
lldp faststart-count 70.5
lldp holdtime-multiplier 70.6
lldp management-address 70.7
lldp med-notifications 70.8
lldp med-tlv-select 70.9
lldp non-strict-med-tlv-order-check 70.11
lldp notification-interval 70.12
lldp notifications 70.13
lldp port-number-type 70.14
lldp reinit 70.15
lldp run 70.16
lldp timer 70.17
lldp tlv-select 70.18
lldp transmit receive 70.20
lldp tx-delay 70.21
location civic-location configuration 70.22
location civic-location identifier 70.26
location civic-location-id 70.27
location coord-location configuration 70.28
location coord-location identifier 70.30
location coord-location-id 70.31
location elin-location 70.32
location elin-location-id 70.33
show debugging lldp 70.34
show lldp 70.35
show lldp interface 70.37
show lldp local-info 70.39
show lldp neighbors 70.43
show lldp neighbors detail 70.45
show lldp statistics 70.48
show lldp statistics interface 70.49
show location 70.51

Introduction

LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (**"Public MIBs" on page 68.83**). The Voice VLAN feature can be configured using commands in **Chapter 17, VLAN Commands**. For more information about LLDP, see **Chapter 69, LLDP, LLDP-MED and Voice VLAN Introduction and Configuration**.

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (**Chapter 66, SNMP Introduction**, **Chapter 67, SNMP Commands**).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.

Command List

This chapter contains an alphabetical list of commands used to configure LLDP.

clear lldp statistics

This command clears all LLDP statistics (packet and event counters) associated with specified ports. If no port list is supplied, LLDP statistics for all ports are cleared.

Syntax `clear lldp statistics [interface <port-list>]`

Parameter	Description
<port-list>	The ports for which the statistics are to be cleared.

Mode Privileged Exec

Examples To clear the LLDP statistics on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp statistics interface port1.0.1,port1.0.6
```

To clear all LLDP statistics for all ports, use the command:

```
awplus# clear lldp statistics
```

Related Commands **show lldp statistics**
show lldp statistics interface

clear lldp table

This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

Syntax `clear lldp table [interface <port-list>]`

Parameter	Description
<port-list>	The ports for which the neighbor information table is to be cleared.

Mode Privileged Exec

Examples To clear the table of neighbor information received on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp table interface port1.0.1,port1.0.6
```

To clear the entire table of neighbor information received through all ports, use the command:

```
awplus# clear lldp table
```

Related Commands **show lldp neighbors**

debug lldp

This command enables specific LLDP debug for specified ports. When LLDP debugging is enabled, diagnostic messages are entered into the system log. If no port list is supplied, the specified debugging is enabled for all ports.

The **no** variant of this command disables specific LLDP debug for specified ports. If no port list is supplied, the specified debugging is disabled for all ports.

Syntax

```
debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]
debug lldp operation
no debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]
no debug lldp operation
no debug lldp all
```

Parameter	Description
`rx`	LLDP receive debug.
`rxpkt`	Raw LLDPDUs received in hex format.
`tx`	LLDP transmit debug.
`txpkt`	Raw Tx LLDPDUs transmitted in hex format.
`<port-list>`	The ports for which debug is to be configured.
`operation`	Debug for LLDP internal operation on the switch.
`all`	Disables all LLDP debugging for all ports.

Default By default no debug is enabled for any ports.

Mode Privileged Exec

Examples To enable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# debug lldp rx interface port1.0.1,port1.0.6
```

To enable debugging of LLDP transmit with packet dump on all ports, use the command:

```
awplus# debug lldp tx txpkt
```

To disable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# no debug lldp rx interface port1.0.1,port1.0.6
```

To turn off all LLDP debugging on all ports, use the command:

```
awplus# no debug lldp all
```

Related Commands
show debugging lldp
show running-config lldp
terminal monitor

lldp faststart-count

Use this command to set the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it starts sending LLDP-MED advertisements from the port, for instance, when it detects a new LLDP-MED capable device.

The **no** variant of this command resets the LLDPD-MED fast start count to the default (3).

Syntax

```
lldp faststart-count <1-10>
no lldp faststart-count
```

Parameter	Description
<1-10>	The number of fast start advertisements to send.

Default The default fast start count is 3.

Mode Global Configuration

Examples To set the fast start count to 5, use the command:

```
awplus# configure terminal
awplus(config)# lldp faststart-count 5
```

To reset the fast start count to the default setting (3), use the command:

```
awplus# configure terminal
awplus(config)# no lldp faststart-count
```

Related Commands show lldp

lldp holdtime-multiplier

This command sets the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.

The **no** variant of this command sets the multiplier back to its default.

Syntax

```
lldp holdtime-multiplier <2-10>
no lldp holdtime-multiplier
```

Parameter	Description
<2-10>	The multiplier factor.

Default The default holdtime multiplier value is 4.

Mode Global Configuration

Usage The Time-To-Live defines the period for which the information advertised to the neighbor is valid. If the Time-To-Live expires before the neighbor receives another update of the information, then the neighbor discards the information from its database.

Examples To set the holdtime multiplier to 2, use the commands:

```
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 2
```

To set the holdtime multiplier back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp holdtime-multiplier 2
```

Related Commands show lldp

lldp management-address

This command sets the IPv4 address to be advertised to neighbors (in the Management Address TLV) via the specified ports. This address will override the default address for these ports.

The **no** variant of this command clears the user-configured management IP address advertised to neighbors via the specified ports. The advertised address reverts to the default.

Syntax

```
lldp management-address <ipaddr>
no lldp management-address
```

Parameter	Description
<ipaddr>	The IPv4 address to be advertised to neighbors, in dotted decimal format. This must be one of the IP addresses already configured on the device.

Default The local loopback interface primary IPv4 address if set, else the primary IPv4 interface address of the lowest numbered VLAN the port belongs to, else the MAC address of the device's baseboard if no VLAN IP addresses are configured for the port.

Mode Interface Configuration

Usage To see the management address that will be advertised, use the **show lldp interface** command or **show lldp local-info** command.

Examples To set the management address advertised by ports 1.0.1 and 1.06, to be 192.168.1.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by ports 1.0.1 and 1.0.6, and revert to using the default address, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp management-address
```

Related Commands
show lldp interface
show lldp local-info

lldp med-notifications

Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the **no** variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

Syntax

```
lldp med-notifications
no lldp med-notifications
```

Default The sending of LLDP-MED notifications is disabled by default.

Mode Interface Configuration

Examples To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-notifications
```

To disable the sending of LLDP-MED notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-notifications
```

Related Commands

lldp notification-interval
lldp notifications
snmp-server enable trap
show lldp interface

lldp med-tlv-select

Use this command to enable LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via the specified ports. The LLDP-MED Capabilities TLV must be enabled before any of the other LLDP-MED Organizationally Specific TLVs are enabled.

Use the **no** variant of this command to disable the specified LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via these ports. In order to disable the LLDP-MED Capabilities TLV, you must also disable the rest of these TLVs. Disabling all these TLVs disables LLDP-MED advertisements.

Syntax

```
lldp med-tlv-select {[capabilities] [network-policy] [location]
   [power-management-ext] [inventory-management]}

lldp med-tlv-select all

no lldp med-tlv-select {[capabilities] [network-policy] [location]
   [power-management-ext] [inventory-management]}

no lldp med-tlv-select all
```

Parameter	Description
`capabilities`	LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV from IEEE 802.3 Organizationally Specific TLVs is also automatically included in LLDP-MED advertisements, whether or not it has been explicitly enabled by the **lldp tlv-select** command.
`network-policy`	Network Policy TLV. This TLV is transmitted if Voice VLAN parameters have been configured using the commands: ■ **switchport voice dscp** ■ **switchport voice vlan** ■ **switchport voice vlan priority**
`location`	Location Identification TLV. This TLV is transmitted if location information has been configured using the commands: ■ **location elin-location-id** ■ **location civic-location identifier** ■ **location civic-location configuration** ■ **location coord-location identifier** ■ **location coord-location configuration** ■ **location elin-location**
`power-management-ext`	Extended Power-via-MDI TLV. This TLV is transmitted if the port is PoE capable, and PoE is enabled (**power-inline enable** command on page 23.7).
`inventory-management`	Inventory Management TLV Set, including the following TLVs: ■ Hardware Revision ■ Firmware Revision ■ Software Revision ■ Serial Number ■ Manufacturer Name ■ Model Name ■ Asset ID

Parameter(cont.)	Description(cont.)
`all`	All LLDP-MED Organizationally Specific TLVs.

Default By default LLDP-MED Capabilities, Network Policy, Location Identification and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the **lldp run** command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

Mode Interface Configuration

Usage LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the **show lldp neighbors** command.

Examples To enable inclusion of the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via ports 1.0.1 and 1.0.6, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select all
```

Related Commands
lldp tlv-select
location elin-location-id
location civic-location identifier
location civic-location configuration
location coord-location identifier
location coord-location configuration
location elin-location
show lldp interface
switchport voice dscp
switchport voice vlan
switchport voice vlan priority

lldp non-strict-med-tlv-order-check

Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the **no** variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

Syntax

```
lldp non-strict-med-tlv-order-check
no lldp non-strict-med-tlv-order-check
```

Default By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

Mode Global Configuration

Usage The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

Examples To enable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

Related Commands **show running-config lldp**

lldp notification-interval

This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).

The **no** variant of this command sets the notification interval back to its default.

Syntax

```
lldp notification-interval <5-3600>
no lldp notification-interval
```

Parameter	Description
<5-3600>	The interval in seconds.

Default The default notification interval is 5 seconds.

Mode Global Configuration

Examples To set the notification interval to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp notification-interval 20
```

To set the notification interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp notification-interval
```

Related Commands

lldp notifications
show lldp

lldp notifications

This command enables the sending of LLDP SNMP notifications (traps) relating to specified ports.

The **no** variant of this command disables the sending of LLDP SNMP notifications for specified ports.

Syntax

```
lldp notifications
no lldp notifications
```

Default The sending of LLDP SNMP notifications is disabled by default.

Mode Interface Configuration

Examples To enable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp notifications
```

To disable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp notifications
```

Related Commands

lldp notification-interval
show lldp interface
snmp-server enable trap

lldp port-number-type

This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. The LLDP MIB (*IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions*.) requires the port number value to count LLDP local port entries.

This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.

The **no** variant of this command resets the type of port identifier back to the default setting (number).

Syntax

```
lldp port-number-type [number|ifindex]
no lldp port-number-type
```

Parameter	Description
`number`	Set the type of port identifier to a port number to enumerate the LLDP MIB local port entries.
`ifindex`	Set the type of port identifier to an interface index to enumerate the LLDP MIB local port entries.

Default The default port identifier type is number. The no variant of this command sets the port identifier type to the default.

Mode Global Configuration

Examples To set the type of port identifier used to enumerate LLDP MIB local port entries to port numbers, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type number
```

To set the type of port identifier used to enumerate LLDP MIB local port entries to interface indexes, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type ifindex
```

To reset the type of port identifier used to enumerate LLDP MIB local port entries the default (port numbers), use the commands:

```
awplus# configure terminal
awplus(config)# no lldp port-number-type
```

Related Commands **show lldp**

lldp reinit

This command sets the value of the reinitialization delay. This is the minimum time after disabling LLDP on a port before it can reinitialize.

The **no** variant of this command sets the reinitialization delay back to its default setting.

Syntax

```
lldp reinit <1-10>
no lldp reinit
```

Parameter	Description
<1-10>	The delay in seconds.

Default The default reinitialization delay is 2 seconds.

Mode Global Configuration

Examples To set the reinitialization delay to 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp reinit 3
```

To set the reinitialization delay back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp reinit
```

Related Commands **show lldp**

lldp run

This command enables the operation of LLDP on the device.

The **no** variant of this command disables the operation of LLDP on the device. The LLDP configuration remains unchanged.

Syntax

```
lldp run
no lldp run
```

Default LLDP is disabled by default.

Mode Global Configuration

Examples To enable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# lldp run
```

To disable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp run
```

Related Commands show lldp

lldp timer

This command sets the value of the transmit interval. This is the interval between regular transmissions of LLDP advertisements.

The **no** variant of this command sets the transmit interval back to its default.

Syntax

```
lldp timer <5-32768>
no lldp timer
```

Parameter	Description
<5-32768>	The transmit interval in seconds. The transmit interval must be at least four times the transmission delay timer (**lldp tx-delay** command).

Default The default transmit interval is 30 seconds.

Mode Global Configuration

Examples To set the transmit interval to 90 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp timer 90
```

To set the transmit interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp timer
```

Related Commands

lldp tx-delay
show lldp

lldp tlv-select

This command enables one or more optional TLVs, or all TLVs, for transmission in LLDP advertisements via the specified ports. The TLVs can be specified in any order; they are placed in LLDP frames in a fixed order (as described in IEEE 802.1AB). The mandatory TLVs (Chassis ID, Port ID, Time To Live, End of LLDPDU) are always included in LLDP advertisements.

In LLDP-MED advertisements the MAC/PHY Configuration/Status TLV will be always be included regardless of whether it is selected by this command.

The **no** variant of this command disables the specified optional TLVs, or all optional TLVs, for transmission in LLDP advertisements via the specified ports.

Syntax

```
lldp tlv-select {[<tlv>]...}
lldp tlv-select all
no lldp tlv-select {[<tlv>]...}
no lldp tlv-select all
```

Parameter	Description
<tlv>	The TLV to transmit in LLDP advertisements. One of these keywords: ■ port-description (specified by the **description (interface)** command on page 12.2) ■ system-name (specified by the **hostname** command on page 8.17) ■ system-description ■ system-capabilities ■ management-address ■ port-vlan ■ port-and-protocol-vlans ■ vlan-names ■ protocol-ids ■ mac-phy-config ■ power-management (Power Via MDI TLV) ■ link-aggregation ■ max-frame-size
`all`	All TLVs.

Default By default no optional TLVs are included in LLDP advertisements. The MAC/PHY Configuration/Status TLV (**mac-phy-config**) is included in LLDP-MED advertisements whether or not it is selected by this command.

Mode Interface Configuration

Examples

To include the management-address and system-name TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select management-address system-name
```

To include all optional TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select all
```

To exclude the management-address and system-name TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select management-address system-name
```

To exclude all optional TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select all
```

Related Commands

description (interface)
hostname
lldp med-tlv-select
show lldp interface
show lldp local-info

lldp transmit receive

This command enables transmission and/or reception of LLDP advertisements to or from neighbors through the specified ports.

The **no** variant of this command disables transmission and/or reception of LLDP advertisements through specified ports.

Syntax

```
lldp {[transmit] [receive]}
no lldp {[transmit] [receive]}
```

Parameter	Description
`transmit`	Enable or disable transmission of LLDP advertisements via this port or ports.
`receive`	Enable or disable reception of LLDP advertisements via this port or ports.

Default LLDP advertisement transmission and reception are enabled on all ports by default.

Mode Interface Configuration

Examples To enable transmission of LLDP advertisements on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp transmit receive
```

Related Commands **show lldp interface**

lldp tx-delay

This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

Syntax

```
lldp tx-delay <1-8192>
no lldp tx-delay
```

Parameter	Description
<1-8192>	The transmission delay in seconds. The transmission delay cannot be greater than a quarter of the transmit interval (**lldp timer** command).

Default The default transmission delay timer is 2 seconds.

Mode Global Configuration

Examples To set the transmission delay timer to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

Related Commands

lldp timer
show lldp

location civic-location configuration

Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the **no** variants of this command to delete civic address parameters from the location.

Syntax

```
country <country>
state <state>
no state
county <county>
no county
city <city>
no city
division <division>
no division
neighborhood <neighborhood>
no neighborhood
street-group <street-group>
no street-group
leading-street-direction <leading-street-direction>
no leading-street-direction
trailing-street-suffix <trailing-street-suffix>
no trailing-street-suffix
street-suffix <street-suffix>
no street-suffix
house-number <house-number>
no house-number
house-number-suffix <house-number-suffix>
no house-number-suffix
landmark <landmark>
no landmark
additional-information <additional-information>
no additional-information
name <name>
no name
postalcode <postalcode>
no postalcode
```

```
building <building>
no building
unit <unit>
no unit
floor <floor>
no floor
room <room>
no room
place-type <place-type>
no place-type
postal-community-name <postal-community-name>
no postal-community-name
post-office-box <post-office-box>
no post-office-box
additional-code <additional-code>
no additional-code
seat <seat>
no seat
primary-road-name <primary-road-name>
no primary-road-name
road-section <road-section>
no road-section
branch-road-name <branch-road-name>
no branch-road-name
sub-branch-road-name <sub-branch-road-name>
no sub-branch-road-name
street-name-pre-modifier <street-name-pre-modifier>
no street-name-pre-modifier
streetname-post-modifier <streetname-post-modifier>
no streetname-post-modifier
```

Parameter	Description
<country>	Upper-case two-letter country code, as specified in *ISO 3166*.
<state>	State (Civic Address (CA) Type 1): national subdivisions (state, canton, region).
<county>	County (CA Type 2): County, parish, gun (JP), district (IN).

Parameter(cont.)	Description(cont.)
<city>	City (CA Type 3): city, township, shi (JP).
<division>	City division (CA Type 4): City division, borough, city district, ward, chou (JP).
<neighborhood>	Neighborhood (CA Type 5): neighborhood, block.
<street-group>	Street group (CA Type 6): group of streets below the neighborhood level.
<leading-street-direction>	Leading street direction (CA Type 16).
<trailing-street-suffix>	Trailing street suffix (CA Type 17).
<street-suffix>	Street suffix (CA Type 18): street suffix or type.
<house-number>	House number (CA Type 19).
<house-number-suffix>	House number suffix (CA Type 20).
<landmark>	Landmark or vanity address (CA Type 21).
<additional-information>	Additional location information (CA Type 22).
<name>	Name (CA Type 23): residence and office occupant.
<postal-code>	Postal/zip code (CA Type 24).
<building>	Building (CA Type 25): structure.
<unit>	Unit (CA Type 26): apartment, suite.
<floor>	Floor (CA Type 27).
<room>	Room (CA Type 28).
<place-type>	Type of place (CA Type 29).
<postal-community-name>	Postal community name (CA Type 30).
<post-office-box>	Post office box (P.O. Box) (CA Type 31).
<additional-code>	Additional code (CA Type 32).
<seat>	Seat (CA Type 33): seat (desk, cubicle, workstation).
<primary-road-name>	Primary road name (CA Type 34).
<road-section>	Road section (CA Type 35).
<branch-road-name>	Branch road name (CA Type 36).
<sub-branch-road-name>	Sub-branch road name (CA Type 37).
<street-name-pre-modifier>	Street name pre-modifier (CA Type 38).
<street-name-post-modifier>	Street name post-modifier (CA Type 39).

Default By default no civic address location information is configured.

Mode Civic Address Location Configuration

Usage The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in *ISO 3166*. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see **"LLDP-MED: Location Identification TLV" on page 69.7**.

To specify the civic address location, use the **location civic-location identifier** command. To delete the civic address location, use the **no** variant of the **location civic-location identifier** command. To assign the civic address location to particular ports, so that it can be advertised in TLVs from those ports, use the command **location civic-location-id** command.

Examples To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

Related Commands
location civic-location-id
location civic-location identifier
show lldp local-info
show location

location civic-location identifier

Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

Syntax

```
location civic-location identifier <civic-loc-id>
no location civic-location identifier <civic-loc-id>
```

Parameter	Description
<civic-loc-id>	A unique civic address location ID, in the range 1 to 4095.

Default By default there are no civic address locations.

Mode Global Configuration

Usage To configure the location information for this civic address location identifier, use the **location civic-location configuration** command. To associate this civic location identifier with particular ports, use the **location elin-location-id** command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

Examples To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

Related Commands
location civic-location-id
location civic-location configuration
show location
show running-config lldp

location civic-location-id

Use this command to assign a civic address location to the ports. The civic address location must already exist. This replaces any previous assignment of civic address location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location civic-location-id <civic-loc-id>
no location civic-location-id [<civic-loc-id>]
```

Parameter	Description
<civic-loc-id>	Civic address location ID, in the range 1 to 4095.

Default By default no civic address location is assigned to ports.

Mode Interface Configuration

Usage The civic address location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, create the location using the following commands:

- **location civic-location identifier** command
- **location civic-location configuration** command

If a civic-address location is deleted using the **no** variant of the **location civic-location identifier** command, it is automatically removed from all ports.

Examples To assign the civic address location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location civic-location-id 1
```

To remove a civic address location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location civic-location-id
```

Related Commands

lldp med-tlv-select
location civic-location identifier
location civic-location configuration
show location

location coord-location configuration

Use this command to configure a coordinate-based location. All parameters must be configured before assigning this location identifier to a port.

Syntax

```
latitude <latitude>
lat-resolution <lat-resolution>
longitude <longitude>
long-resolution <long-resolution>
altitude <altitude> {meters|floor}
alt-resolution <alt-resolution>
datum {wgs84|nad83-navd|nad83-mllw}
```

Parameter	Description
<lat-resolution>	Latitude resolution, as a number of valid bits, in the range 0 to 34.
<latitude>	Latitude value in degrees in the range -90.0 to 90.0
<long-resolution>	Longitude resolution, as a number of valid bits, in the range 0 to 34.
<longitude>	Longitude value in degrees, in the range -180.0 to 180.0.
<alt-resolution>	Altitude resolution, as a number of valid bits, in the range 0 to 30. A resolution of 0 can be used to indicate an unknown value.
<altitude>	Altitude value, in meters or floors.
`meters`	The altitude value is in meters.
`floors`	The altitude value is in floors.
`datum`	The geodetic system (or datum) that the specified coordinate values are based on.
`wgs84`	World Geodetic System 1984.
`nad83-navd`	North American Datum 1983 - North American Vertical Datum.
`nad83-mllw`	North American Datum 1983 - Mean Lower Low Water vertical datum.

Default By default no coordinate location information is configured.

Mode Coordinate Configuration

Usage Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise altitude is stored as a 30-bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be

represented exactly—the stored binary number is converted to a decimal number for display in the output of the **show location** command. For example, a user-entered latitude value of "2.77" degrees is displayed as "2.769999980926513671875000".

The **lat-resolution**, **long-resolution**, and **alt-resolution** parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the **location coord-location identifier** command. To remove coordinate information, delete the coordinate location by using the **no** variant of that command. To associate the coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the **location elin-location-id** command.

Example To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# la-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# lo-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

Related Commands
location coord-location-id
location coord-location identifier
show lldp local-info
show location

location coord-location identifier

Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

Syntax

```
location coord-location identifier <coord-loc-id>
no location coord-location identifier <coord-loc-id>
```

Parameter	Description
<coord-loc-id>	A unique coordinate location identifier, in the range 1 to 4095.

Default By default there are no coordinate locations.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To configure this coordinate location, use the **location coord-location configuration** command. To associate this coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the **location coord-location-id** command.

Examples To enter Coordinate Location Configuration mode to configure the coordinate location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)#
```

To delete coordinate location 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location coord-location identifier 1
```

Related Commands

location coord-location-id
location coord-location configuration
show lldp local-info
show location

location coord-location-id

Use this command to assign a coordinate location to the ports. The coordinate location must already exist. This replaces any previous assignment of coordinate location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location from the ports.

Syntax

```
location coord-location-id <coord-loc-id>
no location coord-location-id [<coord-loc-id>]
```

Parameter	Description
<coord-loc-id>	Coordinate location ID, in the range 1 to 4095.

Default By default no coordinate location is assigned to ports.

Mode Interface Configuration

Usage The coordinate location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the following commands:

- **location coord-location identifier** command
- **location coord-location configuration** command

If a coordinate location is deleted using the **no** variant of the **location coord-location identifier** command, it is automatically removed from all ports.

Examples To assign coordinate location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location coord-location-id 1
```

To remove a coordinate location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location coord-location-id
```

Related Commands

lldp med-tlv-select
location coord-location identifier
location coord-location configuration
show location

location elin-location

Use this command to create or modify an ELIN location.

Use the **no** variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

Syntax

```
location elin-location <elin> identifier <elin-loc-id>
no location elin-location identifier <elin-loc-id>
```

Parameter	Description
<elin>	Emergency Location Identification Number (ELIN) for Emergency Call Service (ECS), in the range 10 to 25 digits long. In North America, ELINs are typically 10 digits long.
<elin-loc-id>	A unique ELIN location identifier, in the range 1 to 4095.

Default By default there are no ELIN location identifiers.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To assign this ELIN location to particular ports, so that it can be advertised in TLVs from those ports, use the **location elin-location-id** command.

Examples To create a new ELIN location with ID 1, and configure it with ELIN "1234567890", use the commands:

```
awplus# configure terminal
awplus(config)# location elin-location 1234567890 identifier 1
```

To delete existing ELIN location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location elin-location identifier 1
```

Related Commands

location elin-location-id
show lldp local-info
show location

location elin-location-id

Use this command to assign an ELIN location to the ports. The ELIN location must already exist. This replaces any previous assignment of ELIN location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location elin-location-id <elin-loc-id>
no location elin-location-id [<elin-loc-id>]
```

Parameter	Description
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.

Default By default no ELIN location is assigned to ports.

Mode Interface Configuration

Usage An ELIN location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the **location elin-location** command.

If an ELIN location is deleted using the **no** variant of one of the **location elin-location** command, it is automatically removed from all ports.

Examples To assign ELIN location 1 to port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location elin-location-id 1
```

To remove an ELIN location from port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location elin-location-id
```

Related Commands

lldp med-tlv-select
location elin-location
show location

show debugging lldp

This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

Syntax `show debugging lldp [interface <port-list>]`

Parameter	Description
<port-list>	The ports for which the LLDP debug settings are shown.

Mode User Exec and Privileged Exec

Examples To display LLDP debug settings for all ports, use the command:

```
awplus# show debugging lldp
```

To display LLDP debug settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show debugging lldp interface port1.0.1-1.0.6
```

Output **Figure 70-1: Example output from the show debugging lldp command**

```
LLDP Debug settings:
Debugging for LLDP internal operation is on
Port       Rx    RxPkt   Tx    TxPkt
-----------------------------------
1.0.1      Yes   Yes     No    No
1.0.2      Yes   No      No    No
1.0.3      No    No      No    No
1.0.4      Yes   Yes     Yes   No
1.0.5      Yes   No      Yes   No
1.0.6      Yes   Yes     Yes   Yes
```

Table 70-1: Parameters in the output of the show debugging lldp command

Parameter	Description
Port	Port name.
Rx	Whether debugging of LLDP receive is enabled on the port.
RxPkt	Whether debugging of LLDP receive packet dump is enabled on the port.
Rx	Whether debugging of LLDP transmit is enabled on the port.
RxPkt	Whether debugging of LLDP transmit packet dump is enabled on the port.

Related Commands debug lldp

show lldp

This command displays LLDP status and global configuration settings.

Syntax `show lldp`

Mode User Exec and Privileged Exec

Example To display LLDP status and global configuration settings, use the command:

```
awplus# show lldp
```

Output

Figure 70-2: Example output from the show lldp command

```
awplus# show lldp

LLDP Global Configuration:              [Default Values]
LLDP Status ............... Enabled     [Disabled]
Notification Interval ..... 5 secs      [5]
Tx Timer Interval ......... 30 secs     [30]
Hold-time Multiplier ...... 4           [4]
(Computed TTL value ....... 120 secs)
Reinitialization Delay .... 2 secs      [2]
Tx Delay .................. 2 secs      [2]
Port Number Type........... Ifindex     [Port-Number]
Fast Start Count .......... 5           [3]

LLDP Global Status:
Total Neighbor Count ...... 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

Table 70-2: Parameters in the output of the show lldp command

Parameter	Description
LLDP Status	Whether LLDP is enabled. Default is disabled.
Notification Interval	Minimum interval between LLDP notifications.
Tx Timer Interval	Transmit interval between regular transmissions of LLDP advertisements.
Hold-time Multiplier	The holdtime multiplier. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.
Reinitialization Delay	The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.
Tx Delay	The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information.
Port Number Type	The type of port identifier used to enumerate LLDP MIB local port entries, as set by the lldp port-number-type command.
Fast Start Count	The number of times fast start advertisements are sent for LLDP-MED.

Table 70-2: Parameters in the output of the show lldp command(cont.)

Parameter	Description
`Total Neighbor Count`	Number of LLDP neighbors discovered on all ports.
`Neighbors table last updated`	The time since the LLDP neighbor table was last updated.

Related Commands

show lldp interface
show running-config lldp

show lldp interface

This command displays LLDP configuration settings for specified ports. If no port list is specified, LLDP configuration for all ports is displayed.

Syntax `show lldp interface [<port-list>]`

Parameter	Description
<port-list>	The ports for which the LLDP configuration settings are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP configuration settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show lldp interface port1.0.1-1.0.6
```

To display LLDP configuration settings for all ports, use the command:

```
awplus# show lldp interface
```

Output **Figure 70-3: Example output from the show lldp interface command**

```
awplus# show lldp interface port1.0.1-1.0.6
LLDP Port Status and Configuration:

  * = LLDP is inactive on this port because it is a mirror analyser port
  Notification Abbreviations:
    RC = LLDP Remote Tables Change       TC = LLDP-MED Topology Change
  TLV Abbreviations:
    Base:  Pd = Port Description         Sn = System Name
           Sd = System Description       Sc = System Capabilities
           Ma = Management Address
    802.1: Pv = Port VLAN ID             Pp = Port And Protocol VLAN ID
           Vn = VLAN Name                Pi = Protocol Identity
    802.3: Mp = MAC/PHY Config/Status    Po = Power Via MDI (PoE)
           La = Link Aggregation         Mf = Maximum Frame Size
    MED:   Mc = LLDP-MED Capabilities    Np = Network Policy
           Lo = Location Identification  Pe = Extended PoE    In = Inventory

                                          Optional TLVs Enabled for Tx
 Port     Rx/Tx  Notif  Management Addr  Base       802.1    802.3    MED
-------------------------------------------------------------------------------
 1.0.1    Rx Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
*1.0.2    -- Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
 1.0.3    Rx Tx  RC --  192.168.100.123  Pd--SdScMa PvPpVnPi -------- McNpLoPe--
 1.0.4    -- --  RC --  192.168.100.123  PdSnSd--Ma -------- -------- McNpLoPe--
 1.0.5    Rx Tx  RC TC  192.168.100.123  PdSnSdScMa PvPpVnPi -------- McNpLoPe--
 1.0.6    Rx Tx  RC TC  192.168.100.123  Pd----ScMa -------- -------- McNpLoPe--
```

Table 70-3: Parameters in the output of the show lldp interface command

Parameter	Description
`Port`	Port name.
`Rx`	Whether reception of LLDP advertisements is enabled on the port.

Table 70-3: Parameters in the output of the show lldp interface command(cont.)

Parameter(cont.)	Description (cont.)
`Tx`	Whether transmission of LLDP advertisements is enabled on the port.
`Notif`	Whether sending SNMP notification for LLDP is enabled on the port: ■ RM = Remote Tables Change Notification ■ TP = LLDP-MED Topology Change Notification
`Management Addr`	Management address advertised to neighbors.
`Base TLVs Enabled for Tx`	List of optional Base TLVs enabled for transmission: ■ Pd = Port Description ■ Sn =System Name ■ Sd = System Description ■ Sc =System Capabilities ■ Ma = Management Address
`802.1 TLVs Enabled for Tx`	List of optional 802.1 TLVs enabled for transmission: ■ Pv = Port VLAN ID ■ Pp = Port And Protocol VLAN ID ■ Vn = VLAN Name ■ Pi =Protocol Identity
`802.3 TLVs Enabled for Tx`	List of optional 802.3 TLVs enabled for transmission: ■ Mp = MAC/PHY Configuration/Status ■ Po = Power Via MDI (PoE) ■ La = Link Aggregation ■ Mf = Maximum Frame Size
`MED TLVs Enabled for Tx`	List of optional LLDP-MED TLVs enabled for transmission: ■ Mc = LLDP-MED Capabilities ■ Np = Network Policy ■ Lo = Location Information, ■ Pe = Extended Power-Via-MDI ■ In = Inventory

Related Commands

show lldp
show running-config lldp

show lldp local-info

This command displays local LLDP information that can be transmitted through specified ports. If no port list is entered, local LLDP information for all ports is displayed.

Syntax

```
show lldp local-info [base] [dot1] [dot3] [med] [interface
   <port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 802.3 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the local information is to be shown.

Mode User Exec and Privileged Exec

Usage Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements (**lldp transmit receive** command)
- which TLVs it is configured to send (**lldp tlv-select** command, **lldp med-tlv-select** command)

Examples To display local information transmitted via port 1.0.1, use the command:

```
awplus# show lldp local-info interface port1.0.1
```

To display local information transmitted via all ports, use the command:

```
awplus# show lldp local-info
```

Output **Figure 70-4: Example output from the show lldp local-info command**

```
LLDP Local Information:

Local port1.0.1:
  Chassis ID Type ..................... MAC address
  Chassis ID .......................... 0015.77c9.7453
  Port ID Type ........................ Interface alias
  Port ID ............................. port1.0.1
  TTL ................................. 120
  Port Description .................... [not configured]
  System Name ......................... awplus
  System Description .................. Allied Telesis router/switch, AW+
                                        v5.4.3A
  System Capabilities - Supported .. Bridge, Router
                      - Enabled .... Bridge, Router
  Management Address .................. 192.168.1.6
  Port VLAN ID (PVID) ................. 1
  Port & Protocol VLAN - Supported . Yes
                       - Enabled ... No
                       - VIDs ..... 0
  VLAN Names .......................... default
  Protocol IDs ........................ 9000, 0026424203000000, 888e01, aaaa03,
                                        88090101, 00540000e302, 0800, 0806, 86dd
  MAC/PHY Auto-negotiation ......... Supported, Enabled
       Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                     10BaseTFD, 10BaseT
       Operational MAU Type ........ 1000BaseTFD (30)
  Power Via MDI (PoE) ............... Supported, Enabled
       Port Class .................. PSE
       Pair Control Ability ........ Disabled
       Power Class ................. Unknown
  Link Aggregation .................. Supported, Disabled
  Maximum Frame Size ................ 1522
  LLDP-MED Device Type .............. Network Connectivity
  LLDP-MED Capabilities ............. LLDP-MED Capabilities, Network Policy,
                                     Location Identification,
                                     Extended Power - PSE, Inventory
  Network Policy .................... [not configured]
  Location Identification .......... Civic Address
       Country Code ................ NZ
       City ........................ Christchurch
       Street Suffix ............... Avenue
       House Number ................ 27
       Primary Road Name ........... Nazareth
  Location Identification .......... ELIN
       ELIN ........................ 123456789012
  Extended Power Via MDI (PoE) ..... PSE
       Power Source ................ Primary Power
       Power Priority .............. Low
       Power Value ................. 4.4 Watts
  Inventory Management:
       Hardware Revision ........... A-0
       Firmware Revision ........... 1.1.0
       Software Revision ........... v5.4.3A
       Serial Number ............... G1Q78900B
       Manufacturer Name ........... Allied Telesis Inc.
       Model Name .................. x610-48Ts/XP
       Asset ID .................... [zero length]
```

Table 70-4: Parameters in the output of the show lldp local-info command

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the local device.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the local port through which advertisements are sent.
`TTL`	Number of seconds that the information advertised by the local port remains valid.
`Port Description`	Port description of the local port, as specified by the **description (interface)** command on page 12.2.
`System Name`	System name, as specified by the **hostname** command on page 8.17.
`System Description`	System description.
`System Capabilities (Supported)`	Capabilities that the local port supports.
`System Capabilities (Enabled)`	Enabled capabilities on the local port.
`Management Addresses`	Management address associated with the local port. To change this, use the **lldp management-address** command.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames received via the local port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLANs (PPV) is supported on the local port.
`Port & Protocol VLAN (Enabled)`	Whether the port is in one or more Port & Protocol VLANs.
`Port & Protocol VLAN (VIDs)`	List of identifiers for Port & Protocol VLANs that the port is in.
`VLAN Names`	List of VLAN names for VLANs that the local port is assigned to.
`Protocol IDs`	List of protocols that are accessible through the local port.
`MAC/PHY Auto-negotiation`	Auto-negotiation support and current status of the 802.3 LAN on the local port.
`Power Via MDI (PoE)`	PoE-capability and current status on the local port.
`Port Class`	Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device)

Table 70-4: Parameters in the output of the show lldp local-info command(cont.)

Parameter	Description
`Pair Control Ability`	Whether power pair selection can be controlled
`Power Pairs`	Which power pairs are selected for power ("Signal Pairs" or "Spare Pairs") if pair selection can be controlled
`Power Class`	The power class of the PD device on the port (class 0, 1, 2, 3 or 4)
`Link Aggregation`	Whether the link is capable of being aggregated and it is currently in an aggregation.
`Aggregated Port-ID`	Aggregated port identifier.
`Maximum Frame Size`	The maximum frame size capability of the implemented MAC and PHY.
`LLDP-MED Device Type`	LLDP-MED device type
`LLDP-MED Capabilities`	Capabilities LLDP-MED capabilities supported on the local port.
`Network Policy`	List of network policies configured on the local port.
`VLAN ID`	VLAN identifier for the port for the specified application type
`Tagged Flag`	Whether the VLAN ID is to be used as tagged or untagged
`Layer-2 Priority:`	Layer 2 User Priority (in the range 0 to 7)
`DSCP Value`	Diffserv codepoint (in the range 0 to 63)
`Location Identification`	Location configured on the local port.
`Extended Power Via MDI (PoE)`	PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.
`Power Source`	The power source the switch currently uses; either primary power or backup power.
`Power Priority`	The power priority configured on the port; either critical, high or low.
`Power Value`	The total power the switch can source over a maximum length cable to a PD device on the port. The value shows the power value in Watts from the PD side.
`Inventory Management`	Inventory information for the device.

Related Commands

description (interface)
hostname
lldp transmit receive

show lldp neighbors

This command displays a summary of information received from neighbors via specified ports. If no port list is supplied, neighbor information for all ports is displayed.

Syntax `show lldp neighbors [interface <port-list>]`

Parameter	Description
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors
```

To display neighbor information received via ports 1.0.1 and 1.0.6 with LLDP-MED configuration, use the command:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.6
```

Output **Figure 70-5: Example output from the show lldp neighbors command**

```
LLDP Neighbor Information:

Total number of neighbors on these ports .... 4

  System Capability Codes:
    O = Other    P = Repeater   B = Bridge                W = WLAN Access Point
    R = Router   T = Telephone  C = DOCSIS Cable Device   S = Station Only
  LLDP-MED Device Type and Power Source Codes:
    1 = Class I    3 = Class III    PSE  = PoE    Both = PoE&Local   Prim = Primary
    2 = Class II   N = Network Con. Locl = Local  Unkn = Unknown     Back = Backup

Local    Neighbor         Neighbor        Neighbor                 System      MED
Port     Chassis ID       Port ID         Sys Name                 Cap.        Ty Pwr
-------------------------------------------------------------------------------
1.0.1    002d.3044.7ba6   port1.0.2       awplus                   OPBWRTCS
1.0.1    0011.3109.e5c6   port1.0.3       AT-9924 switch/route...  --B-R---
1.0.6    0000.10cf.8590   port3           AR-442S                  --B-R---
1.0.6    00ee.4352.df51   192.168.1.2     Jim's desk phone         --B--T--    3  PSE
```

Table 70-5: Parameters in the output of the show lldp neighbors command

Parameter	Description
`Local Port`	Local port on which the neighbor information was received.
`Neighbor Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Neighbor Port Name`	Port ID of the neighbor.
`Neighbor Sys Name`	System name of the LLDP neighbor.

Table 70-5: Parameters in the output of the show lldp neighbors command(cont.)

Parameter	Description
`Neighbor Capability`	Capabilities that are supported and enabled on the neighbor.
`System Capability`	System Capabilities of the LLDP neighbor.
`MED Device Type`	LLDP-MED Device class (Class I, II, III or Network Connectivity)
`MED Power Source`	LLDP-MED Power Source

Related Commands show lldp neighbors detail

show lldp neighbors detail

This command displays in detail the information received from neighbors via specified ports. If no port list is supplied, detailed neighbor information for all ports is displayed.

Syntax

```
show lldp neighbors detail [base] [dot1] [dot3] [med] [interface
   <port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 803.1 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display detailed neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors detail
```

To display detailed neighbor information received via ports 1.0.1, use the command:

```
awplus# show lldp neighbors detail interface port1.0.1
```

Output **Figure 70-6: Example output from the show lldp neighbors detail command**

```
awplus# show lldp neighbors detail interface port1.0.1
LLDP Detailed Neighbor Information:

Local port1.0.1:
  Neighbors table last updated 0 hrs 0 mins 40 secs ago

  Chassis ID Type ................... MAC address
  Chassis ID ........................ 0004.cd28.8754
  Port ID Type ...................... Interface alias
  Port ID ........................... port1.0.6
    TTL ............................. 120 (secs)
  Port Description .................. [zero length]
  System Name ....................... awplus
  System Description ................ Allied Telesis router/switch, AW+ v5.4.4
  System Capabilities - Supported .. Bridge, Router
                      - Enabled .... Bridge, Router
  Management Addresses .............. 0004.cd28.8754
  Port VLAN ID (PVID) ............... 1
  Port & Protocol VLAN - Supported . Yes
                       - Enabled ... Yes
                       - VIDs ...... 5
  VLAN Names ........................ default, vlan5
  Protocol IDs ...................... 9000, 0026424203000000, 888e01, 8100,
                                      88090101, 00540000e302, 0800, 0806, 86dd
  MAC/PHY Auto-negotiation ......... Supported, Enabled
       Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                      10BaseTFD, 10BaseT
       Operational MAU Type ........ 1000BaseTFD (30)
  Power Via MDI (PoE) ............... [not advertised]
  Link Aggregation .................. Supported, Disabled
  Maximum Frame Size ................ 1522 (Octets)
  LLDP-MED Device Type .............. Network Connectivity
  LLDP-MED Capabilities ............. LLDP-MED Capabilities, Network Policy,
                                      Location Identification,
                                      Extended Power - PSE, Inventory
  Network Policy .................... [not advertised]
  Location Identification ........... [not advertised]
  Extended Power Via MDI (PoE) ..... PD
           Power Source ............. PSE
           Power Priority ........... High
           Power Value .............. 4.4 Watts
  Inventory Management:
           Hardware Revision ........ X1-0
           Firmware Revision ........ 1.1.0
           Software Revision ........ v5.4.4
           Serial Number ............ M1NB73008
           Manufacturer Name ........ Allied Telesis Inc.
           Model Name ............... AT-GS924MPX
           Asset ID ................. [zero length]
```

Table 70-6: Parameters in the output of the show lldp neighbors detail command

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the neighbor.
`TTL`	Number of seconds that the information advertised by the neighbor remains valid.
`Port Description`	Port description of the neighbor's port.

Table 70-6: Parameters in the output of the show lldp neighbors detail

Parameter	Description
`System Name`	Neighbor's system name.
`System Description`	Neighbor's system description.
`System Capabilities (Supported)`	Capabilities that the neighbor supports.
`System Capabilities (Enabled)`	Capabilities that are enabled on the neighbor.
`Management Addresses`	List of neighbor's management addresses.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames for the neighbor port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLAN is supported on the LLDP neighbor.
`Port & Protocol VLAN (Enabled)`	Whether Port & Protocol VLAN is enabled on the LLDP neighbor.
`Port & Protocol VLAN (VIDs)`	List of Port & Protocol VLAN identifiers.
`VLAN Names`	List of names of VLANs that the neighbor's port belongs to.
`Protocol IDs`	List of protocols that are accessible through the neighbor's port.
`MAC/PHY Auto-negotiation`	Auto-negotiation configuration and status
`Power Via MDI (PoE)`	PoE configuration and status of 802.3 Power-Via-MDI TLV
`Link Aggregation`	Link aggregation information
`Maximum Frame Size`	The maximum frame size capability
`LLDP-MED Device Type`	LLDP-MED Device type
`LLDP-MED Capabilities`	LLDP-MED capabilities supported
`Network Policy`	List of network policies
`Location Identification`	Location information
`Extended Power Via MDI (PoE)`	PoE-capability and current status
`Inventory Management`	Inventory information

Related Commands **show lldp neighbors**

show lldp statistics

This command displays the global LLDP statistics (packet and event counters).

Syntax `show lldp statistics`

Mode User Exec and Privileged Exec

Example To display global LLDP statistics information, use the command:

```
awplus# show lldp statistics
```

Output

Figure 70-7: Example output from the show lldp statistics command

```
awplus# show lldp statistics

Global LLDP Packet and Event counters:

  Frames:     Out ................... 345
              In .................... 423
              In Errored ............ 0
              In Dropped ............ 0
  TLVs:       Unrecognized .......... 0
              Discarded ............. 0
  Neighbors:  New Entries ........... 20
              Deleted Entries ....... 20
              Dropped Entries ....... 0
              Entry Age-outs ........ 20
```

Table 70-7: Parameters in the output of the show lldp statistics command

Parameter	Description
`Frames Out`	Number of LLDPDU frames transmitted.
`Frames In`	Number of LLDPDU frames received.
`Frames In Errored`	Number of invalid LLDPDU frames received.
`Frames In Dropped`	Number of LLDPDU frames received and discarded for any reason.
`TLVs Unrecognized`	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
`TLVs Discarded`	Number of LLDP TLVs discarded for any reason.
`Neighbors New Entries`	Number of times the information advertised by neighbors has been inserted into the neighbor table.
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related Commands clear lldp statistics
show lldp statistics interface

show lldp statistics interface

This command displays the LLDP statistics (packet and event counters) for specified ports. If no port list is supplied, LLDP statistics for all ports are displayed.

Syntax `show lldp statistics interface [<port-list>]`

Parameter	Description
<port-list>	The ports for which the statistics are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP statistics information for all ports, use the command:

```
awplus# show lldp statistics interface
```

To display LLDP statistics information for ports 1.0.1 and 1.0.6, use the command:

```
awplus# show lldp statistics interface port1.0.1,port1.0.6
```

Output

Figure 70-8: Example output from the show lldp statistics interface command

```
awplus# show lldp statistics interface port1.0.1,port1.0.6

LLDP Packet and Event Counters:

port1.0.1
  Frames:     Out ................... 27
              In .................... 22
              In Errored ............ 0
              In Dropped ............ 0
  TLVs:       Unrecognized .......... 0
              Discarded ............. 0
  Neighbors:  New Entries ........... 3
              Deleted Entries ....... 0
              Dropped Entries ....... 0
              Entry Age-outs ........ 0

port1.0.6
  Frames:     Out ................... 15
              In .................... 18
              In Errored ............ 0
              In Dropped ............ 0
  TLVs:       Unrecognized .......... 0
              Discarded ............. 0
  Neighbors:  New Entries ........... 1
              Deleted Entries ....... 0
              Dropped Entries ....... 0
              Entry Age-outs ........ 0
```

Table 70-8: Parameters in the output of the show lldp statistics interface command

Parameter	Description
`Frames Out`	Number of LLDPDU frames transmitted.
`Frames In`	Number of LLDPDU frames received.

Table 70-8: Parameters in the output of the show lldp statistics interface

Parameter	Description
`Frames In Errored`	Number of invalid LLDPDU frames received.
`Frames In Dropped`	Number of LLDPDU frames received and discarded for any reason.
`TLVs Unrecognized`	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
`TLVs Discarded`	Number of LLDP TLVs discarded for any reason.
`Neighbors New Entries`	Number of times the information advertised by neighbors has been inserted into the neighbor table.
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related Commands

clear lldp statistics
show lldp statistics

show location

Use this command to display selected location information configured on the switch.

Syntax

```
show location {civic-location|coord-location|elin-location}

show location {civic-location|coord-location|elin-location}
   identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}

show location {civic-location|coord-location|elin-location} interface
   <port-list>
```

Parameter	Description
`civic-location`	Display civic location information.
`coord-location`	Display coordinate location information.
`elin-location`	Display ELIN location information.
<civic-loc-id>	Civic address location identifier, in the range 1 to 4095.
<coord-loc-id>	Coordinate location identifier, in the range 1 to 4095.
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.
<port-list>	Ports to display information about.

Mode User Exec and Privileged Exec

Examples To display a civic address location configured on port1.0.1, use the command:

```
awplus# show location civic-location interface port1.0.1
```

Figure 70-9: Example output from the show location command

```
awplus# show location civic-location interface port1.0.1
Port     ID   Element Type          Element Value
-------------------------------------------------------------
1.0.1    1    Country               NZ
              City                  Christchurch
              Street-suffix         Avenue
              House-number          27
              Primary-road-name     Nazareth
```

To display coordinate location information configured on the identifier 1, use the command:

```
awplus# show location coord-location identifier 1
```

Figure 70-10: Example output from the show location command

```
awplus# show location coord-location identifier 1
  ID  Element Type             Element Value
------------------------------------------------------------------
  1   Latitude Resolution      15 bits
      Latitude                 38.898648113012313842773437 5 degrees
      Longitude Resolution     15 bits
      Longitude                130.232323229312896728515625 0 degrees
      Altitude Resolution      10 bits
      Altitude                 2.50000000 meters
      Map Datum                WGS 84
```

The coordinate location information displayed may differ from the information entered because it is stored in binary format. For more information, see the **location coord-location configuration** command.

To display all ELIN location information configured on the switch, use the command:

```
awplus# show location elin-location
```

Figure 70-11: Example output from the show location command

```
awplus# show location elin-location
  ID  ELIN
-----------------------------------
  1   1234567890
  2   5432154321
```

Related Commands

location elin-location-id
location civic-location identifier
location civic-location configuration
location coord-location identifier
location coord-location configuration
location elin-location

Chapter 71: SMTP Commands

Command List 71.2
debug mail 71.2
delete mail 71.3
mail 71.4
mail from 71.5
mail smtpserver 71.6
show counter mail 71.7
show mail 71.8
undebug mail 71.8

Command List

This chapter provides an alphabetical reference for commands used to configure SMTP.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

debug mail

This command turns on debugging for sending emails.

The **no** variant of this command turns off debugging for sending emails.

Syntax

```
debug mail
no debug mail
```

Mode Privileged Exec

Examples To turn on debugging for sending emails, use the command:

```
awplus# debug mail
```

To turn off debugging for sending emails, use the command:

```
awplus# no debug mail
```

Related Commands

delete mail
mail
mail from
mail smtpserver
show mail
show counter mail
undebug mail

delete mail

This command deletes mail from the queue.

Syntax `delete mail [mail-id <mail-id>|all]`

Parameter	Description	
`mail-id`	Deletes a single mail from the mail queue.	
	<mail-id>	An unique mail ID number. Use the **show mail** command to display this for an item of mail.
`all`	Delete all the mail in the queue.	

Mode Privileged Exec

Examples To delete a unique mail item `20060912142356.1234` from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

Related Commands
debug mail
mail
mail from
mail smtpserver
show mail

mail

This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the **mail from** command and a mail server using the **mail smtpserver** command.

Syntax `mail [{to <to>|subject <subject>|file <filename>}]`

Parameter	Description
`to`	The email recipient.
	`<to>` Email address.
`subject`	Description of the subject of this email. Use quote marks when the subject text contains spaces.
	`<subject>` String.
`file`	File to insert as text into the message body.
	`<filename>` String.

Mode Privileged Exec

Example To send an email to `rei@nerv.com` with the subject `dummy plug configuration`, and with the message body inserted from the file `plug.conf` use the command:

```
awplus# mail rei@nerv.com subject dummy plug configuration
        filename plug.conf
```

Related Commands
debug mail
delete mail
mail from
mail smtpserver
show mail
show counter mail

mail from

This command sets an email address for the “mail from” SMTP command. You must specify a sending email address with this command before you can send any email.

Syntax `mail from <from>`

Parameter	Description
<from>	The email address that the mail is sent from.

Mode Global Configuration

Example To set the email address you are sending mail from to “kaji@nerv.com, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

Related Commands
delete mail
mail
mail smtpserver
show mail

mail smtpserver

This command sets the IP address of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send any email.

Syntax `mail smtpserver <ip-address>`

Parameter	Description
<ip-address>	Internet Protocol (IP) Address for the mail server specified.

Mode Global Configuration

Example To specify a mail server at 192.168.0.1, use the command:

```
awplus# mail smtpserver 192.168.0.1
```

Related Commands
debug mail
delete mail
mail
mail from
show mail
show counter mail

show counter mail

This command displays the mail counters.

Syntax `show counter mail`

Mode User Exec and Privileged Exec

Output **Figure 71-1: Example output from the show counter mail command**

```
Mail Client (SMTP) counters
Mails Sent            ......... 0
Mails Sent Fails      ......... 1
```

Table 71-1: Parameters in the output of the show counter mail command

Parameter	Description
`Mails Sent`	The number of emails sent successfully since the last device restart.
`Mails Sent Fails`	The number of emails the device failed to send since the last device restart.

Example To show the emails in the queue use the command:

```
awplus# show counter mail
```

Related Commands
debug mail
delete mail
mail
mail from
show mail

show mail

This command displays the emails in the queue.

Syntax `show mail`

Mode Privileged Exec

Example To display the emails in the queue use the command:

```
awplus# show mail
```

Related Commands **delete mail**
mail
show counter mail

undebug mail

This command applies the functionality of the no **debug mail** command on page 71.2.

Chapter 72: RMON Introduction and Configuration

Introduction 72.2
Overview 72.2
RMON Configuration Example 72.3

Introduction

The chapter describes the Remote Network MONitoring (RMON) service on the switch, and describes a configuration example showing how to set up an RMON alarm.

This RMON alarm configuration example described creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port exceeds a threshold, and creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch drops below a lower threshold.

For detailed information about the commands used to configure RMON, see **Chapter 73, RMON Commands**

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

Overview

The Remote Network MONitoring (RMON) MIB (RFC2819) was developed by the IETF to support monitoring and protocol analysis of LANs with a focus on Layer 1 and 2 information in networks. RMON is an industry standard that provides the functionality in network analyzers.

An RMON implementation operates in a client/server model. Monitoring devices (or 'probes') contain RMON agents that collect information and analyze packets. The probes are servers and the Network Management applications that communicate with them are clients. While agent configuration and data collection uses SNMP, RMON operates differently than SNMP systems:

- Probes have responsibility for data collection and processing, reducing SNMP traffic and reducing processing load for clients.
- Information is only transmitted to the management application when required, not polled.

RMON is mainly used for 'flow-based' monitoring, while SNMP is mainly used for 'device-based' management. RMON data collected deals mainly with traffic patterns on the network, and SNMP data collected usually deals with the status of individual devices on the network.

One disadvantage of flow based monitoring is that remote devices have much more of the management burden, and require more resources. AlliedWare Plus minimizes the management and resources burden by implementing a subset of the RMON MIB group to provide a minimal RMON agent implementation supporting statistics, history, alarms, and events.

The RMON groups supported in AlliedWare Plus™ are:

- **Statistics** - collects Ethernet statistics on a switch port, such as utilization and collisions.
- **History** - collects a history of Ethernet statistics on a switch port.
- **Alarms** - monitor a MIB object for a specified interval, trigger an alarm at a specified value (the '**rising threshold**'), and resets the alarm at another value (the '**falling threshold**'). Alarms are used with events to trigger alarms, which generate logs or SNMP traps.
- **Events** - specify the action to take when an event is triggered by an alarm.

  The action of an event can generate a log or an SNMP trap.

RMON Configuration Example

This configuration example sets up an RMON alarm to create SNMP traps and log messages. This RMON alarm creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port exceeds a threshold, and creates SNMP traps and log messages when the rate of receipt of Broadcast packets on a switch port drops below a lower threshold.

Step 1: Set up an RMON collection on the switch port that is being monitored.

Use the following commands to configure this functionality:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# rmon collection stats 4
```

This will cause the software to build a table in which it stores statistics relating to the switch port.

Step 2: Define an RMON event that will be called by the alarm when the thresholds are passed.

Create this as a 'trap and log' event, so that both an SNMP trap and a log message will be generated. The trap will be sent to the SNMP community named 'public'.

Use the following command to configure this functionality:

```
awplus# configure terminal
awplus(config)# rmon event 10 log trap public
```

Step 3: Create the RMON alarm.

Every 5 seconds, the alarm checks the broadcast packet counter in RMON collection stats 4. If the change in the value of that counter over the 5 second interval exceeds 5000 (1000 broadcasts per second), the alarm will trigger the event defined in step 2 above.

Additionally, when the rate broadcast falls below 500 broadcasts per 5 seconds, then the alarm will trigger the event defined in step 2 above again.

Use the below command to configure this functionality:

```
awplus# configure terminal
awplus(config)# rmon alarm 5 etherStatsBroadcastPkts.4
                interval 5 delta
                rising-threshold 5000 event 10
                falling-threshold 500 event 10
                alarmstartup 3
```

For the variable '`etherStatsBroadcastPkts.4`' in this command, note that '`.4`' refers to the index number of the RMON collection stats 4 as defined on `port1.0.4`.

So, '`etherStatsBroadcastPkts.4`' refers to 'Received broadcasts' in RMON collection stats 4. Further counters for RMON are defined in section 5 of RFC 1757.

Step 4: Enable RMON traps.

To ensure that the SNMP trap is sent, you need to enabled RMON traps, and you need to define a trap host in SNMP. Use the below commands to configure this functionality:

```
awplus# configure terminal
awplus(config)# snmp-server
awplus(config)# snmp-server enable trap rmon
awplus(config)# snmp-server community public
awplus(config)# snmp-server host 192.168.2.254 version 2c
public
```

Note that the resulting log message will be of the form listed below:

```
RMON [1024]: Alarm Index 5 alarm Rising Threshold 5000 alarm
Value 5117 alarm Rising event Index 10 event description
RMON_SNMP
```

Chapter 73: RMON Commands

Command List 73.2
rmon alarm 73.2
rmon collection history 73.4
rmon collection stats 73.5
rmon event 73.6
show rmon alarm 73.7
show rmon event 73.8
show rmon history 73.9
show rmon statistics 73.10

Command List

This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see **Chapter 72, RMON Introduction and Configuration**

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

rmon alarm

Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the **rmon event** command.

Use the **no** variant of this command to remove the alarm configuration.

Note Only alarms for switch port interfaces, not for VLAN interfaces, can be configured.

Syntax

```
rmon alarm <alarm-index> <oid> interval <1-2147483647> {delta|
   absolute} rising-threshold <1-2147483647> event <rising-event-
   index> falling-threshold <1-2147483647> event <falling-event-
   index> alarmstartup {1|2|3} [owner <owner>]

no rmon alarm <alarm-index>
```

Parameter	Description
<alarm-index>	*<1-65535>* Alarm entry index value.
<oid>	The variable SNMP MIB Object Identifier (OID) name to be monitored, in the format etherStatsEntry.field.<*stats-index*>. For example, etherStatsEntry.5.22 is the OID for the etherStatsPkts field in the etherStatsEntry table for the interface defined by the <*stats-index*> 22 in the **rmon collection stats** command.
`interval <1-2147483647>`	Polling interval in seconds.
`delta`	The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.
`absolute`	The RMON MIB alarmSampleType: the value of the monitored MIB object.

Parameter(cont.)	Description(cont.)
`rising-threshold <1-2147483647>`	Rising threshold value of the alarm entry in seconds.
`<rising-event-index>`	`<1-65535>` The event to be triggered when the monitored object value reaches the rising threshold value. This is an event index of an event specified by the **rmon event** command.
`falling-threshold <1-2147483647>`	Falling threshold value of the alarm entry in seconds.
`<falling-event-index>`	`<1-65535>` The event to be triggered when the monitored object value reaches the falling threshold value. This is an event index of an event specified by the **rmon event** command.
`alarmstartup {1|2|3}`	Whether RMON can trigger a falling alarm (1), a rising alarm (2) or either (3) when you first start monitoring. See the Usage section for more information.
`owner <owner>`	Arbitrary owner name to identify the alarm entry.

Default By default, there are no alarms.

Mode Global Configuration

Usage RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The **alarmstartup** parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that the SNMP MIB Object Identifier (OID) indicated in the command syntax with <***oid***> must be specified as a dotted decimal value with the form **etherStatsEntry.field.**<***stats-index***>.

Example To configure an alarm to monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the **rmon collection stats** command), to trigger event 2 (defined by the **rmon event** command) when it reaches the rising threshold 400, and to trigger event 3 when it reaches the falling threshold 200, and identify this alarm as belonging to Maria, use the commands:

```
awplus# configure terminal
awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60
delta rising-threshold 400 event 2 falling-
threshold 200 event 3 alarmstartup 3 owner
maria
```

Related Commands **rmon collection stats**
rmon event

rmon collection history

Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the **no** variant of this command to remove the specified history control configuration.

Note Only a history for switch port interfaces, not for VLAN interfaces, can be collected.

Syntax

```
rmon collection history <history-index> [buckets <1-65535>]
   [interval <1-3600>] [owner <owner>]

no rmon collection history <history-index>
```

Parameter	Description
<history-index>	*<1-65535>* A unique RMON history control entry index value.
buckets *<1-65535>*	Number of requested buckets to store snapshots. Default 50 buckets.
interval *<1-3600>*	Polling interval in seconds. Default 1800 second polling interval.
owner *<owner>*	Owner name to identify the entry.

Default The default interval is 1800 seconds and the default buckets is 50 buckets.

Mode Interface Configuration

Example To create a history statistics control group to store 200 snapshots with an interval of 500 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection history 200 buckets 500
                  interval 600 owner herbert
```

To disable the history statistics control group, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection history 200
```

rmon collection stats

Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the **no** variant of this command to stop collecting RMON statistics on this switch port.

Note Only statistics for switch port interfaces, not for VLAN interfaces, can be collected.

Syntax

```
rmon collection stats <collection-index> [owner <owner>]
no rmon collection stats <collection-index>
```

Parameter	Description
<collection-index>	*<1-65535>* Give this collection of statistics an index number to uniquely identify it. This is the index to use to access the statistics collected for this switch port.
owner *<owner>*	An arbitrary owner name to identify this statistics collection entry.

Default RMON statistics are not enabled by default.

Mode Interface Configuration

Example To enable the collection of RMON statistics with a statistics index of 200, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To to stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no rmon collection stats 200
```

rmon event

Use this command to create an event definition for a log or a trap or both. The event index for this event can then be referred to by the **rmon alarm** command.

Use the **no** variant of this command to remove the event definition.

Note Only the events for switch port interfaces, not for VLAN interfaces, can be collected.

Syntax

```
rmon event <event-index> [description <description>|owner <owner>|
   trap <trap>]

rmon event <event-index> [log [description <description>|
   owner <owner>|trap <trap>] ]

rmon event <event-index> [log trap [description <description>|
   owner <owner>] ]

no rmon event <event-index>
```

Parameter	Description
<event-index>	*<1-65535>* Unique event entry index value.
log	Log event type.
trap	Trap event type.
log trap	Log and trap event type.
description *<description>*	Event entry description.
owner *<owner>*	Owner name to identify the entry.

Default No event is configured by default.

Mode Global Configuration

Example To create an event definition for a log with an index of 299, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To to remove the event definition, use the command:

```
awplus# configure terminal
awplus(config)# no rmon event 299
```

Related Commands **rmon alarm**

show rmon alarm

Use this command to display the alarms and threshold configured for the RMON probe.

Note Only the alarms for switch port interfaces, not for VLAN interfaces, can be shown.

Syntax `show rmon alarm`

Mode User Exec and Privileged Exec

Example To display the alarms and threshold, use this command:

```
awplus# show rmon alarm
```

Related Commands rmon alarm

show rmon event

Use this command to display the events configured for the RMON probe.

Note Only the events for switch port interfaces, not for VLAN interfaces, can be shown.

Syntax `show rmon event`

Mode User Exec and Privileged Exec

Output **Figure 73-1: Example output from the show rmon event command**

```
awplus#sh rmon event
 event Index = 787
       Description TRAP
        Event type log & trap
          Event community name gopher
       Last Time Sent = 0
       Owner  RMON_SNMP

 event Index = 990
       Description TRAP
        Event type trap
          Event community name teabo
       Last Time Sent = 0
       Owner  RMON_SNMP
```

Note The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Example To display the events configured for the RMON probe, use this command:

```
awplus# show rmon event
```

Related Commands rmon event

show rmon history

Use this command to display the parameters specified on all the currently defined RMON history collections on the device.

Note Only the history for switch port interfaces, not for VLAN interfaces, can be shown.

Syntax `show rmon history`

Mode User Exec and Privileged Exec

Output **Figure 73-2: Example output from the show rmon history command**

```
awplus#sh rmon history
 history index = 56
         data source ifindex = 4501
         buckets requested = 34
        buckets granted = 34
        Interval = 2000
        Owner Andrew

 history index = 458
         data source ifindex = 5004
         buckets requested = 400
        buckets granted = 400
        Interval = 1500
        Owner trev
=======================================================
```

Note The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Example To display the parameters specified on all the currently defined RMON history collections, us the commands:

```
awplus# show rmon history
```

Related Commands rmon collection history

show rmon statistics

Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

Note Only statistics for switch port interfaces, not for VLAN interfaces, can be shown.

Syntax `show rmon statistics`

Mode User Exec and Privileged Exec

Example To display the current values of the statistics for all the RMON statistics collections, us the commands:

```
awplus# show rmon statistics
```

Output **Figure 73-3: Example output from the show rmon statistics command**

```
awplus#show rmon statistics
    rmon collection index 45
    stats->ifindex = 4501
    input packets 1279340, bytes 85858960, dropped 00, multicast packets 1272100
    output packets 7306090, bytes 268724, multicast packets 7305660 broadcast
packets 290
    rmon collection index 679
    stats->ifindex = 5013
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 8554550, bytes 26777324, multicast packets 8546690 broadcast
packets 7720
```

Note The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Related Commands rmon collection stats

Chapter 74: Triggers Introduction

Introduction 74.2
Trigger Facility 74.2
Configuring a Trigger 74.2
Troubleshooting Triggers 74.5

Introduction

This chapter provides information about the Trigger facility on this switch. For specific configuration examples, see **Chapter 75, Triggers Configuration**. For detailed descriptions of the commands used to configure triggers, see **Chapter 76, Trigger Commands**.

Trigger Facility

The Trigger facility provides a powerful mechanism for automatic and timed management of your device by automating the execution of commands in response to certain events. For example, you can use triggers to deactivate a service during the weekends, or to collect diagnostic information when the CPU usage is high.

A **trigger** is an ordered sequence of scripts that is executed when a certain event occurs. A **script** is a sequence of commands stored as a plain text file on a file subsystem accessible to the device, such as Flash memory. Each trigger may reference multiple scripts and any script may be used by any trigger. When an event activates a trigger, the trigger executes the scripts associated with it in sequence. One script is executed completely before the next script begins. Various types of triggers are supported, each activated in a different way.

Configuring a Trigger

The following describes the general steps to configure a trigger. For specific configuration examples, see **Chapter 75, Triggers Configuration**.

Step 1: Create a configuration script

Create a configuration script with the commands you would like executed when the trigger conditions are met. To create the configuration script using the CLI, use the command:

```
awplus# edit [<filename>]
```

Alternatively, you can create a script on a PC then load it onto your device using the copy (URL) command.

Step 2: Enter the trigger configuration mode

You must be in the Global Configuration mode to reach the Trigger Configuration mode. Use the command:

```
awplus# configure terminal
```

To create a trigger, and enter its configuration mode, use the command:

```
awplus(config)# trigger <1-250>
```

Step 3: Set the trigger type

The trigger type determines how the trigger is activated. To set the trigger to activate:

« when CPU usage reaches a certain level, use the command:

```
awplus(config-trigger)# type cpu <1-100> [up|down|any]
```

« when the link status of a particular interface changes, use the command:

```
awplus(config-trigger)# type interface <interface>
                        [up|down|any]
```

« when the RAM usage reaches a certain level, use the command:

```
awplus(config-trigger)# type memory <1-100> [up|down|any]
```

« periodically after a set number of minutes, use the command:

```
awplus(config-trigger)# type periodic <1-1440>
```

« when a ping poll identifies that a target device's status has changed, use the command:

```
awplus(config-trigger)# type ping-poll <1-100> {up|down}
```

« if your device reboots, use the command:

```
awplus(config-trigger)# type reboot
```

« at a specific time of the day, use the command:

```
awplus(config-trigger)# type time <hh:mm>
```

Note that a combined limit of 10 triggers of the type periodic and type time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

Step 4: Set the time and days that the trigger can activate on

By default triggers can activate at any time of the day, on all days. If you want your trigger to activate only during a specific time of the day, use the command:

```
awplus(config-trigger)# time {[after <hh:mm:ss>]
                        [before <hh:mm:ss>]}
```

If you want your trigger to activate only on a specific date, use the command:

```
awplus(config-trigger)# day <1-31> <month> <2000-2035>
```

If you want the trigger to activate only on specific days of the week, use the command:

```
awplus(config-trigger)# day <weekday>
```

Note that you can set either a specific date, or specific weekdays, but not both.

Step 5: Specify how often the trigger can activate

By default, triggers can activate an unlimited number of times, as long as the trigger conditions are met. To set a limit on the number of times a trigger can activate, use the command:

```
awplus(config-trigger)# repeat {forever|no|once|yes|
                        <1-4294967294>}
```

You device maintains two counters that track the number of times a trigger has activated. One counts the total number of times the trigger is activated and is only reset if the device restarts, or when the trigger is destroyed. The other counter tracks the permitted number of repetitions. To reset this counter, use the **repeat** command on page 76.6.

Step 6: Add the script to the trigger

You can add up to five scripts to the trigger. When a trigger is activated, it executes the scripts in sequence, with the lowest numbered script activated first. The first script runs to completion before the next script begins. To add a script, use the command:

```
awplus(config-trigger)# script <1-5> {<filename>}
```

Step 7: Specify a description for the trigger

Specify a description for the trigger, so that you can easily identify the trigger in show commands and log output. Use the command:

```
awplus(config-trigger)# description <description>
```

Step 8: Verify the trigger's configuration

To check the configuration of the trigger, use the command:

```
awplus(config-trigger)# show trigger [<1-250>|counter|
                        full]
```

Troubleshooting Triggers

You can use the trigger diagnostic mode and trigger debugging to test your triggers and troubleshoot any issues.

Diagnostic mode is set per trigger. In this mode the trigger activates if its trigger conditions are met, but does not run any of its scripts. Your device generates a log message to indicate that the trigger was activated. To place a trigger in diagnostic mode, enter the trigger's configuration mode and use the command:

```
awplus(config-trigger)# test
```

To start debugging for triggers, use the command:

```
awplus(config-trigger)# debug trigger
```

This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

Enabling and Disabling

Triggers are enabled by default. This allows the trigger to activate as soon as its trigger conditions are met. If you need to disable a trigger but do not want to delete the trigger, use the command:

```
awplus(config-trigger)# no active
```

To enable the trigger again, use the command:

```
awplus(config-trigger)# active
```

To delete the trigger, use the command:

```
awplus(config-trigger)# no trigger <1-250>
```

Chapter 75: Triggers Configuration

Introduction 75.2
Restrict Internet Access 75.2
Capture Unusual CPU and RAM Activity 75.4
See Daily Statistics 75.6
Turn Off Power to Port LEDs 75.7
Reduce Power Supplied to Ports 75.9
Capture Show Output and Save to a USB Storage Device 75.11
Load a Release File From a USB Storage Device 75.12

Introduction

The chapter describes how to configure triggers to:

- Restrict Internet Access
- **Capture Unusual CPU and RAM Activity**
- **See Daily Statistics**
- **Turn Off Power to Port LEDs**
- **Capture Show Output and Save to a USB Storage Device**

For more information about triggers, see **Chapter 74, Triggers Introduction**. For detailed descriptions of the commands used to configure triggers, see **Chapter 76, Trigger Commands**.

Restrict Internet Access

In the following configuration the ACME company wants to restrict its employees from accessing popular video sharing websites as this is causing bandwidth problems during work hours. The ACME company is happy for workers to access the site after work hours.

Employee PCs at ACME are on vlan2. Two triggers with associated scripts are needed:

- Trigger 1 activates at 8.30am and runs a script called **shutdown.scp**. This script adds commands to restrict access to the specified sites
- Trigger 2 activates at 5.30pm and runs the script called **open.scp**. This script removes the configuration specified by shutdown.scp

1. Create the **shutdown.scp** script

   Create a configuration script using Access Control List commands to restrict users on vlan2 from accessing the specific sites.

2. Create the **open.scp** script

   Create a script to remove the ACL configuration specified in the **shutdown.scp** file.

3. Configure trigger 1

   To create trigger 1, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
```

   Set the trigger to activate at 8:30am, by using the command:

```
awplus(config-trigger)# type time 08:30
```

   Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

   Add the script **shutdown.scp** to the trigger:

```
awplus(config-trigger)# script 1 shutdown.scp
```

Specify a helpful description, such as **Stops access to video sharing sites**. Use the command:

```
awplus(config-trigger)# description Stops access to video
                        sharing sites
```

Change to Global Configuration mode:

```
awplus(config-trigger)# exit
```

4. Configure trigger 2

To create trigger 2, use the command:

```
awplus(config)# trigger 2
```

Set the trigger to activate at 5.30pm:

```
awplus(config-trigger)# type time 17:30
```

Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

Add the script **open.scp** to the trigger:

```
awplus(config-trigger)# script 1 open.scp
```

Specify a helpful description, such as **Access allowed to video sharing sites**. Use the command:

```
awplus(config-trigger)# description Access allowed to video
                        sharing sites
```

5. Verify the configuration

To check the configuration of the triggers, use the commands:

```
awplus# show trigger 1

awplus# show trigger 2
```

Capture Unusual CPU and RAM Activity

The following configuration allows you to troubleshoot high CPU or RAM usage by the device. It uses two triggers to capture show output, and places this output in a file.

- Trigger 3 activates the script cpu-usage.scp when CPU usage is over 90% and can activate up to 5 times
- Trigger 4 activates the script ram-usage.scp when RAM usage is over 95%, and can activate up to 10 times

1. Create the cpu-usage.scp configuration script

Create a script with the appropriate show command:

```
awplus# show cpu | redirect showcpu.txt
```

The output of the **show cpu** command has been redirected into a file. It is not possible to display trigger script output on the terminal. Redirecting the command output to a file means it is available for later inspection.

If the trigger activates on more than one occasion the contents of **showcpu.txt** will be overwritten with the latest output. To keep a full record for all activations of this trigger an ASH shell script can be added to the trigger to manage the output of the configuration script. For example:

```
#!/bin/ash
date >> showcpu_bkup.txt
cat showcpu.txt >> showcpu_bkup.txt
```

This script concatenates that date and time of activation and the contents of **showcpu.txt** onto the end of the backup file **showcpu_bkup.txt** in flash memory.

Note that the files may grow large accumulating data and consume available flash memory.

2. Create the ram-usage.scp configuration script

Create a script with the appropriate show command:

```
awplus# show memory | redirect showmem.txt
```

The output of the **show memory** command has been redirected into a file. It is not possible to display trigger script output on the terminal. Redirecting the command output to a file means it is available for later inspection.

If the trigger activates on more than one occasion the contents of **showcpu.txt** will be overwritten with the latest output. To keep a full record for all activations of this trigger an ASH shell script can be added to the trigger to manage the output of the configuration script. For example:

```
#!/bin/ash
date >> showmem_bkup.txt
cat showmem.txt >> showmem_bkup.txt
```

This script concatenates that date and time of activation and the contents of **showmem.scp** onto the end of the backup file **showmem_bkup.scp** in flash memory.

Note that the files may grow large accumulating data and consume available flash memory.

3. Configure trigger 3

To create trigger 3, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 3
```

Set the trigger to activate when CPU usage exceeds 80%:

```
awplus(config-trigger)# type cpu 90 up
```

Add the script **cpu-usage.scp** to the trigger:

```
awplus(config-trigger)# script 1 cpu-usage.scp
```

Return to Global Configuration mode:

```
awplus(config-trigger)# exit
```

4. Configure trigger 4

To create trigger 4, use the command:

```
awplus(config)# trigger 4
```

Set the trigger to activate when RAM usage exceeds 95%:

```
awplus(config-trigger)# type cpu 95 up
```

Add the script **cpu-usage.scp** to the trigger:

```
awplus(config-trigger)# script 1 ram-usage.scp
```

5. Verify the configuration

To check the configuration of the triggers, use the command:

```
awplus# show trigger 3
awplus# show trigger 4
```

See Daily Statistics

The ACME company has recently set up QoS on its traffic to give traffic different priorities to the ISP. ACME wants to assess how much traffic is dropped with the QoS bandwidths set over the next week. To do this, they want to generate an hourly report on QoS traffic on the first day that this is implemented.

- Trigger 5 activates the script **qos-stats.scp** every 60 minutes.

  The trigger is set to only activate during work hours.

1. Create the **qos-stats.scp** script

Create a configuration script with the appropriate show commands. You can either create the configuration script using the CLI with the **edit** command or create a script on a PC then load it onto your device using the **copy (URL)** command on page 7.16.

2. Configure trigger 5

To create trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
```

Set the trigger to activate periodically every 60 minutes:

```
awplus(config-trigger)# type periodic 60
```

Set the trigger to activate only during the hours of 8:00am and 6:00pm:

```
awplus(config-trigger)# time after 8:00 before 18:00
```

Add the script **qos-stats.scp** to the trigger:

```
awplus(config-trigger)# script 1 qos-stats.scp
```

3. Verify the configuration

To check the configuration of the trigger, use the command:

```
awplus# show trigger 5
```

Turn Off Power to Port LEDs

The following configuration allows you to conserve power by using the eco-friendly LED (Light Emitting Diode) feature to turn off power to the port LEDs during non-work hours.

See the **ecofriendly led** command for a detailed command description and command examples. See the section **"Save Power with the Eco-Friendly Feature" on page 1.32**.

- Trigger 6 activates at 5.30pm and runs a script called **LEDoff.scp**. This script adds commands to turn off power to all the port LEDs
- Trigger 7 activates at 8.30am and runs the script called **LEDon.scp**. This script removes the configuration specified by **LEDoff.scp**

1. Create the **LEDoff.scp** script

Create a configuration script with the commands that are executed when the trigger conditions are met. You can either create the configuration script using the CLI with the edit command or create a script on a PC then load it onto your device using the copy (URL) command. The configuration script for this example is:

```
!
enable
configure terminal
ecofriendly led
exit
exit
!
```

2. Create the **LEDon.scp** script

Create a script to remove the configuration specified in the **LEDoff.scp** file. The configuration script for this example is:

```
!
enable
configure terminal
no ecofriendly led
exit
exit
!
```

3. Configure trigger 6

To create trigger 6, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
```

Set the trigger to activate at 5:30pm, by using the command:

```
awplus(config-trigger)# type time 17:30
```

Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

Add the script **LEDoff.scp** to the trigger:

```
awplus(config-trigger)# script 1 LEDoff.scp
```

Specify a helpful description, such as **Shutdown power to LEDs**. Use the command:

```
awplus(config-trigger)# description Shutdown power to LEDs
```

Change to Global Configuration mode:

```
awplus(config-trigger)# exit
```

4. Configure trigger 7

To create trigger 7, use the command:

```
awplus(config)# trigger 9
```

Set the trigger to activate at 8.30am:

```
awplus(config-trigger)# type time 08:30
```

Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

Add the script **LEDon.scp** to the trigger:

```
awplus(config-trigger)# script 1 LEDon.scp
```

Specify a helpful description, such as **Turn on power to LEDs**. Use the command:

```
awplus(config-trigger)# description Turn on power to LEDs
```

5. Verify the configuration

To check the configuration of the triggers, use the commands:

```
awplus# show trigger 6
awplus# show trigger 7
```

Reduce Power Supplied to Ports

The following configuration allows you to conserve power by using the eco-friendly LPI (Low Power Idle) feature to reduce power supplied to the ports during non-work hours.

See the **ecofriendly lpi** command for a detailed command description and command examples. See the section **"Save Power with the Eco-Friendly Feature" on page 1.32**.

- Trigger 6 activates at 5.30pm and runs a script called **LPIon.scp**. This script adds commands to reduce power to all the ports.
- Trigger 7 activates at 8.30am and runs the script called **LPIoff.scp**. This script removes the configuration specified by **LPIon.scp**.

1. Create the **LPIon.scp** script

Create a configuration script with the commands that are executed when the trigger conditions are met. You can either create the configuration script using the CLI with the edit command or create a script on a PC then load it onto your device using the copy (URL) command. The configuration script for this example is:

```
!
enable
configure terminal
ecofriendly lpi
exit
exit
!
```

2. Create the **LPIoff.scp** script

Create a script to remove the configuration specified in the **LPIon.scp** file. The configuration script for this example is:

```
!
enable
configure terminal
no ecofriendly lpi
exit
exit
!
```

3. Configure trigger 6

To create trigger 6, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
```

Set the trigger to activate at 5:30pm, by using the command:

```
awplus(config-trigger)# type time 17:30
```

Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

Add the script **LPIon.scp** to the trigger:

```
awplus(config-trigger)# script 1 LPIon.scp
```

Specify a helpful description, such as **Turn on LPI**. Use the command:

```
awplus(config-trigger)# description Turn on LPI
```

Change to Global Configuration mode:

```
awplus(config-trigger)# exit
```

4. Configure trigger 7

To create trigger 7, use the command:

```
awplus(config)# trigger 9
```

Set the trigger to activate at 8.30am:

```
awplus(config-trigger)# type time 08:30
```

Set the trigger to activate on Monday, Tuesday, Wednesday, Thursday and Friday:

```
awplus(config-trigger)# day mon tue wed thur fri
```

Add the script **LPIoff.scp** to the trigger:

```
awplus(config-trigger)# script 1 LPIoff.scp
```

Specify a helpful description, such as **Turn off LPI**. Use the command:

```
awplus(config-trigger)# description Turn off LPI
```

5. Verify the configuration

To check the configuration of the triggers, use the commands:

```
awplus# show trigger 6
awplus# show trigger 7
```

Capture Show Output and Save to a USB Storage Device

The following configuration allows you to automatically capture output from the show tech-support command when a USB storage device is inserted into the switch. It uses a script called by the USB storage device trigger to capture the **show tech-support** output and places this output in a file on the USB storage device.

- Trigger 9 activates the script **shtech-sup.scp** when a USB storage device is inserted in the switch

1. Create the **shtech-sup.scp** script

Create a configuration script with the commands that are executed when the trigger conditions are met. You can either create the configuration script using the CLI with the edit command or create a script on a PC then load it onto your device using the copy (URL) command. The configuration script for this example is:

```
!
enable
show tech-support outfile usb:support.txt.gz
exit
end
!
```

2. Configure trigger 9

To create trigger 9, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 9
```

Set the trigger to activate on the insertion of a USB storage device:

```
awplus(config-trigger)# type usb in
```

Add the script **shtech-sup.scp** to the trigger:

```
awplus(config-trigger)# script 1 shtech-sup.scp
```

3. Verify the configuration

To check the configuration of the triggers, use the command:

```
awplus# show trigger 9
```

Load a Release File From a USB Storage Device

The following configuration allows you to automatically load a release file from a USB storage device into Flash memory when a USB storage device is inserted into the switch. It uses a script called by the USB trigger to load the release file from the USB storage device.

Note that you can only specify that the release file is on a USB storage device if there is a backup release file already specified in Flash. See the **boot system backup** command for further information.

Caution **Anyone with physical access to the switch and who knows the name of the release file loaded by the trigger could insert a USB storage device and overwrite the boot configuration in Flash memory.**

- Trigger 11 activates the script **copy.scp** when a USB storage device is inserted in the switch

1. Create the **copy.scp** script

Create a configuration script with the commands that are executed when the trigger conditions are met. You can either create the configuration script using the CLI with the edit command or create a script on a PC then load it onto your device using the copy (URL) command. The configuration script for this example is:

```
!
enable
copy usb flash GS900-5.4.4E-1.1.rel
wait 5
configure terminal
boot system GS900-5.4.4E-1.1.rel
exit
end
!
```

2. Configure trigger 11

To create trigger 11, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 11
```

Set the trigger to activate on the insertion of a USB storage device:

```
awplus(config-trigger)# type usb in
```

Add the script **copy.scp** to the trigger:

```
awplus(config-trigger)# script 1 copy.scp
```

Specify a helpful description, such as **Load a release file**. Use the command:

```
awplus(config-trigger)# description Load a release file
```

After a USB storage device has been inserted in the switch, use the following two steps to check the trigger and current boot configuration details.

1. Verify the trigger configuration

To check the configuration of the trigger, use the command:

```
awplus# show trigger 11
```

Example output from this command is shown below:

```
awplus#show trigger 11
Trigger Configuration Details
-------------------------------------------------------------
Trigger ..................... 11
Description ................. Load a release file
Type and details ............ USB (in)
Days ........................ smtwtfs
After ....................... 00:00:00
Before ...................... 23:59:59
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... Continuous
Modified .................... Wed Sep 15 16:25:33 2010
Number of activations ....... 1
Last activation ............. Wed Sep 15 16:26:49 2010
Number of scripts ........... 1
  1. copy.scp
  2. <not configured>
  3. <not configured>
  4. <not configured>
  5. <not configured>
-------------------------------------------------------------
```

2. Display the current boot configuration

To display the current boot configuration, use the command:

```
awplus# show boot
```

Example output from this command is shown below:

```
awplus#show boot
Boot configuration
-------------------------------------------------------------
Current software   : GS900-5.4.4E-1.1.rel
Current boot image : flash:/GS900-5.4.4E-1.1.rel
Backup  boot image : flash:/GS900-5.4.4E-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/atplab.cfg (file exists)
Backup  boot config: flash:/default.cfg (file exists)
```

Chapter 76: Trigger Commands

Command List 76.2
active (trigger) 76.2
day 76.3
debug trigger 76.4
description (trigger) 76.5
repeat 76.6
script 76.7
show debugging trigger 76.9
show running-config trigger 76.9
show trigger 76.10
test 76.15
time (trigger) 76.16
trap 76.18
trigger 76.19
trigger activate 76.20
type atmf node 76.21
type cpu 76.23
type interface 76.24
type memory 76.25
type periodic 76.26
type ping-poll 76.27
type reboot 76.27
type stack disabled-master 76.28
type stack link 76.29
type stack master-fail 76.30
type stack member 76.31
type time 76.32
type usb 76.33
undebug trigger 76.33

Command List

This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see **Chapter 74, Triggers Introduction** and **Chapter 75, Triggers Configuration**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

active (trigger)

This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

Syntax

```
active
no active
```

Mode Trigger Configuration

Usage Configure a trigger first before you use this command to activate it. See the **Configuring a Trigger** section in **Chapter 74, Triggers Introduction** for trigger configuration steps.

Examples To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

Related Commands **show trigger**
trigger

day

This command specifies the days or date that the can trigger activate on. You can specify either:

- A specific date
- A specific day of the week
- A list of days of the week
- every day

By default, the trigger can activate on any day.

Syntax

```
day every-day
day <1-31> <month> <2000-2035>
day <weekday>
```

Parameter	Description
`every-day`	Sets the trigger so that it can activate on any day.
<1-31>	Day of the month the trigger is permitted to activate on.
<month>	Sets the month that the trigger is permitted to activate on. Valid keywords are: **january, february, march, april, may, june, july, august, september, october, november**, and **december**.
<2000-2035>	Sets the year that the trigger is permitted to activate in.
<weekday>	Sets the days of the week that the trigger can activate on. You can specify one or more week days in a space separated list. Valid keywords are: **monday, tuesday, wednesday, thursday, friday, saturday**, and **sunday**.

Mode Trigger Configuration

Usage For example trigger configurations that use the **day** command, see **"Restrict Internet Access" on page 75.2** and **"Turn Off Power to Port LEDs" on page 75.7**.

Examples To permit trigger 55 to activate on the `1 Jun 2010`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 Jun 2010
```

To permit trigger 12 to activate on a Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

Related Commands

show trigger
trigger

debug trigger

This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

Syntax

```
debug trigger
no debug trigger
```

Mode Privilege Exec

Examples To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

Related Commands

show debugging trigger
show trigger
test
trigger
undebug trigger

description (trigger)

This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The **no** variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	A word or phrase that uniquely identifies this trigger or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters.

Mode Trigger Configuration

Examples To give trigger 240 the description `daily status report`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 240
awplus(config-trigger)# description daily status report
```

To remove the description from trigger `36`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 36
awplus(config-trigger)# no description
```

Related Commands

show trigger
test
trigger

repeat

This command specifies the number of times that a trigger is permitted to activate. This allows you to specify whether you want the trigger to activate:

- only the first time that the trigger conditions are met
- a limited number of times that the trigger conditions are met
- an unlimited number of times

Once the trigger has reached the limit set with this command, the trigger remains in your configuration but cannot be activated. Use the **repeat** command again to reset the trigger so that it is activated when its trigger conditions are met.

By default, triggers can activate an unlimited number of times. To reset a trigger to this default, specify either **yes** or **forever**.

Syntax `repeat {forever|no|once|yes|<1-4294967294>}`

Parameter	Description
`yes|forever`	The trigger repeats indefinitely, or until disabled.
`no|once`	The trigger activates only once.
<1-4292967294>	The trigger repeats the set number of times.

Mode Trigger Configuration

Examples To allow trigger `21` to activate only once, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 21
awplus(config-trigger)# repeat no
```

To allow trigger `22` to activate an unlimited number of times whenever its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 22
awplus(config-trigger)# repeat forever
```

To allow trigger `23` to activate only the first `10` times the conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 23
awplus(config-trigger)# repeat 10
```

Related Commands **show trigger**
trigger

script

This command specifies one or more scripts that are to be run when the trigger activates. You can add up to five scripts to a single trigger.

The sequence in which the trigger runs the scripts is specified by the number you set before the name of the script file. One script is executed completely before the next script begins.

Scripts may be either ASH shell scripts, indicated by a **.sh** filename extension suffix, or AlliedWare Plus™ scripts, indicated by a **.scp** filename extension suffix. AlliedWare Plus™ scripts only need to be readable.

The **no** variant of this command removes one or more scripts from the trigger's script list. The scripts are identified by either their name, or by specifying their position in the script list. The **all** parameter removes all scripts from the trigger.

Syntax

```
script <1-5> {<filename>}
no script {<1-5>|<filename>|all}
```

Parameter	Description
<1-5>	The position of the script in execution sequence. The trigger runs the lowest numbered script first.
<filename>	The path to the script file.

Mode Trigger Configuration

Examples To configure trigger 71 to run the script flash:/cpu_trig.sh in position 3 when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# script 3 flash:/cpu_trig.sh
```

To configure trigger 99 to run the scripts **flash:reconfig.scp**, **flash:cpu_trig.sh** and **flash:email.scp** in positions 2, 3 and 5 when the trigger activates, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 99
awplus(config-trigger)# script 2 flash:/reconfig.scp 3 flash:/
cpu_trig.sh 5 flash:/email.scp
```

To remove the scripts 1, 3 and 4 from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script 1 3 4
```

To remove the script flash:/cpu_trig.sh from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script flash:/cpu_trig.sh
```

To remove all the scripts from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script all
```

Related Commands

show trigger
trigger

show debugging trigger

This command displays the current status for trigger utility debugging. Use this command to show when trigger debugging has been turned on or off from the **debug trigger** command.

Syntax `show debugging trigger`

Mode User Exec and Privileged Exec

Example To display the current configuration of trigger debugging, use the command:

```
awplus# show debugging trigger
```

Output **Figure 76-1: Example output from the show debugging trigger command**

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is off
```

Related Commands **debug trigger**

show running-config trigger

This command displays the current running configuration of the trigger utility.

Syntax `show running-config trigger`

Mode Privileged Exec

Example To display the current configuration of the trigger utility, use the command:

```
awplus# show running-config trigger
```

Output **Figure 76-2: Example output from the show running-config trigger command**

```
trigger 1
 type usb in
trigger 2
 type usb out
!
```

Related Commands **show trigger**

show trigger

This command displays configuration and diagnostic information about the triggers configured on the device. Specify the **show trigger** command without any options to display a summary of the configuration of all triggers.

Syntax `show trigger [<1-250>|counter|full]`

Parameter	Description
<1-250>	Displays detailed information about a specific trigger, identified by its trigger ID.
`counter`	Displays statistical information about all triggers.
`full`	Displays detailed information about all triggers.

Mode Privileged Exec

Example To get summary information about all triggers, use the following command:

```
awplus# show trigger
```

Figure 76-3: Example output from the show trigger command

```
awplus#show trigger
TR# Type & Details       Name                 Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 USB (in)                                  Y  N  Y  Continuous  0   smtwtfs
002 USB (out)                                 Y  N  Y  Continuous  0   smtwtfs
003 CPU (80% any)        Busy CPU             Y  N  Y  5           1   smtwtfs
005 Periodic (30 min)    Regular status check Y  N  N  Continuous  1   -mtwtf-
007 Memory (85% up)      High mem usage       Y  N  Y  8           1   smtwtfs
011 Time (00:01)         Weekend access       Y  N  Y  Continuous  1   ------s
013 Reboot                                    Y  N  Y  Continuous  2   smtwtfs
017 Interface (vlan1 ... Change config for... Y  N  Y  Once        1   2-apr-2008
019 Ping-poll (5 up)     Connection to svr1   Y  N  Y  Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Table 76-1: Parameters in the output of the show trigger command

Parameter	Description
`TR#`	Trigger identifier (ID).
`Type & Details`	The trigger type, followed by the trigger details in brackets.
`Name`	Descriptive name of the trigger configured with the **description (trigger)** command.
`Ac`	Whether the trigger is active (Y), or inactive (N).
`Te`	Whether the trigger is in test mode (Y) or not (N).
`Tr`	Whether or not the trigger is enabled to send SNMP traps. See the **trap** command.

Table 76-1: Parameters in the output of the show trigger command(cont.)

Parameter	Description
Repeat	Whether the trigger repeats continuously, and if not, the configured repeat count for the trigger. To see the number of times a trigger has activated, use the **show trigger <1-250>** command.
#Scr	Number of scripts associated with the trigger.
Days/Date	Days or date when the trigger may be activated. For the days options, the days are shown as a seven character string representing Sunday to Saturday. A hyphen indicates days when the trigger cannot be activated.

To display detailed information about trigger 3, use the command:

```
awplus# show trigger 3
```

Figure 76-4: Example output from the show trigger command for a specific trigger

```
awplus#show trigger 3
Trigger Configuration Details
-------------------------------------------------------------
Trigger ..................... 1
Description ................. display cpu usage when pass 80%
Type and details ............ CPU (80% up)
Days ........................ 26-nov-2007
After ....................... 00:00:00
Before ...................... 23:59:59
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... 123 (0)
Modified .................... Tue Dec 20 02:26:03 1977
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 1
  1. shocpu.scp
  2. <not configured>
  3. <not configured>
  4. <not configured>
  5. <not configured>
-------------------------------------------------------------
```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Figure 76-5: Example output from the show trigger full command

```
awplus#show trigger full
Trigger Configuration Details
-------------------------------------------------------------
 Trigger ..................... 1
 Description ................. <no description>
 Type and details ............ USB (in)
 Days ........................ smtwtfs
 After ....................... 00:00:00
 Before ...................... 23:59:59
 Active ...................... Yes
 Test ........................ No
 Trap ........................ Yes
 Repeat ...................... Continuous
 Modified .................... Fri Sep  3 14:45:56 2010
 Number of activations ....... 0
 Last activation ............. not activated
 Number of scripts ........... 0
   1. <not configured>
   2. <not configured>
   3. <not configured>
   4. <not configured>
   5. <not configured>

 Trigger ..................... 2
 Description ................. <no description>
 Type and details ............ USB (out)
 Days ........................ smtwtfs
 After ....................... 00:00:00
 Before ...................... 23:59:59
 Active ...................... Yes
 Test ........................ No
 Trap ........................ Yes
 Repeat ...................... Continuous
 Modified .................... Fri Sep  3 14:45:56 2010
 Number of activations ....... 0
 Last activation ............. not activated
 Number of scripts ........... 0
   1. <not configured>
   2. <not configured>
   3. <not configured>
   4. <not configured>
   5. <not configured>

Trigger ..................... 3
Description ................. Busy CPU
Type and details ............ CPU (80% up)
Days ........................ smtwtfs
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... Continuous
Modified .................... Fri Feb 2 17:05:16 2007
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 2
  1. flash:/cpu_alert.sh
  2. flash:/reconfig.scp
  3. <not configured>
  4. <not configured>
  5. <not configured>
-------------------------------------------------------------
```

Table 76-2: Parameters in the output of the show trigger full and show trigger commands for a specific trigger

Parameter	Description
`Trigger`	The ID of the trigger.
`Description`	Descriptive name of the trigger.
`Type and details`	The trigger type and its activation conditions.
`Days`	The days on which the trigger is permitted to activate.
`Date`	The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces “Days”.
`Active`	Whether or not the trigger is permitted to activate.
`Test`	Whether or not the trigger is operating in diagnostic mode.
`Trap`	Whether or not the trigger is enabled to send SNMP traps.
`Repeat`	Whether the trigger repeats an unlimited number of times (Continuous) or for a set number of times. When the trigger can repeat only a set number of times, then the number of times the trigger has been activated is displayed in brackets.
`Modified`	The date and time of the last time that the trigger was modified.
`Number of activations`	Number of times the trigger has been activated since the last restart of the device.
`Last activation`	The date and time of the last time that the trigger was activated.
`Number of scripts`	How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

Figure 76-6: Example output from the show trigger counter command

```
awplus#show trigger counter
Trigger Module Counters
-------------------------------------------------------
Trigger activations ........................... 0
Time triggers activated today ................. 0
Periodic triggers activated today ............. 0
Interface triggers activated today ............ 0
Resource triggers activated today ............. 0
Reboot triggers activated today ............... 0
Ping-poll triggers activated today ............ 0
Stack master fail triggers activated today .... 0
Stack member triggers activated today ......... 0
-------------------------------------------------------
```

Table 76-3: Parameters in the output of the show trigger counter command

Parameter	Description
`Trigger activations`	Number of times a trigger has been activated.
`Time triggers activated today`	Number of times a time trigger has been activated today.
`Periodic triggers activated today`	Number of times a periodic trigger has been activated today.
`Interface triggers activated today`	Number of times an interface trigger has been activated today.
`Resource triggers activated today`	Number of times a CPU or memory resource trigger has been activated today.
`Ping-poll triggers activated today`	Number of times a ping-poll trigger has been activated today.

Related Commands **trigger**

test

This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates the scripts associated with the trigger will be run, as normal.

Syntax

```
test
no test
```

Mode Trigger Configuration

Usage Configure a trigger first before you use this command to diagnose it. See the **Configuring a Trigger** section in **Chapter 74, Triggers Introduction** for trigger configuration steps.

Examples To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

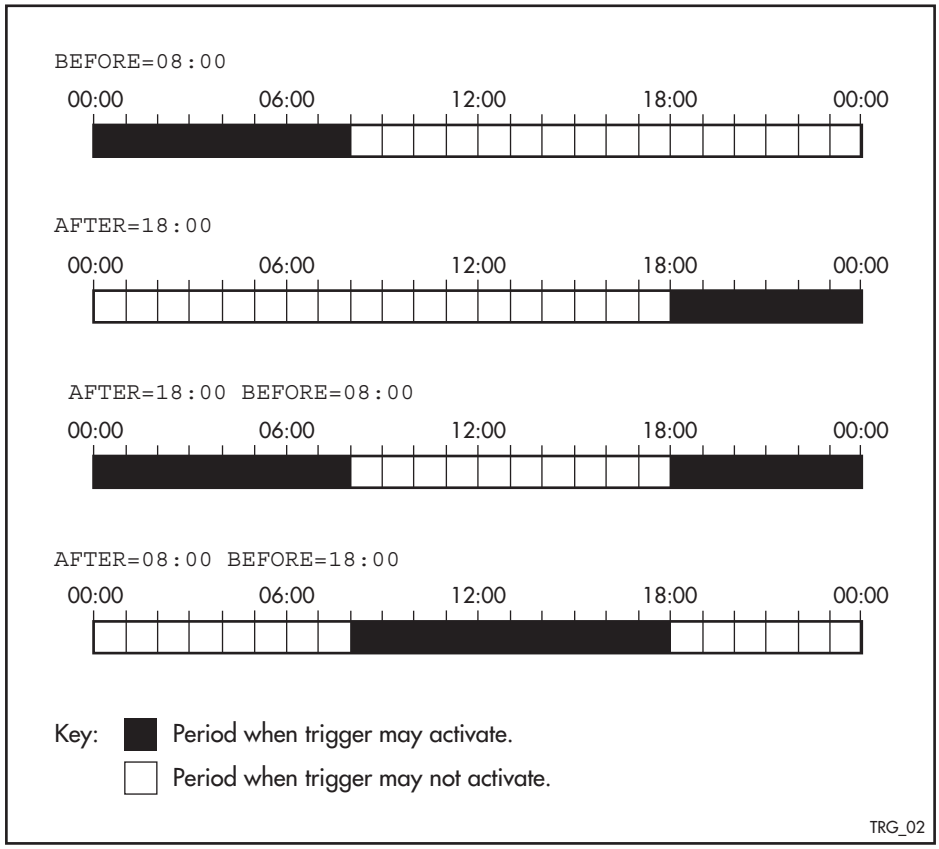
```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

Related Commands **show trigger**
trigger

time (trigger)

This command specifies the time of day when the trigger is permitted to activate. The after parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from "after" to "before" is defined, during which the trigger may activate. This command is not applicable to time triggers (**type time**).

The following figure illustrates how the **before** and **after** parameters operate.



Syntax `time {[after <hh:mm:ss>] [before <hh:mm:ss>]}`

Parameter	Description
`after <hh:mm:ss>`	The earliest time of day when the trigger may be activated.
`before <hh:mm:ss>`	The latest time of day when the trigger may be activated.

Mode Trigger Configuration

Usage For example trigger configurations that use the **time (trigger)** command, see **"Restrict Internet Access" on page 75.2** and **"Turn Off Power to Port LEDs" on page 75.7**.

Examples To allow trigger `63` to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger `64` to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger `65` to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

Related Commands **show trigger**
trigger

trap

This command enables the specified trigger to send SNMP traps.

Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

Syntax

```
trap
no trap
```

Default SNMP traps are enabled by default for all defined triggers.

Mode Trigger Configuration

Usage You must configure SNMP before using traps with triggers. See the following SNMP chapters:

Chapter 66, SNMP Introduction

Chapter 67, SNMP Commands

Chapter 68, SNMP MIBs

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to **AT-TRIGGER-MIB** for further information about the relevant SNMP MIB.

Examples To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

Related Commands

trigger
show trigger

trigger

This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

Syntax

```
trigger <1-250>
no trigger <1-250>
```

Parameter	Description
<1-250>	A trigger ID.

Mode Global Configuration

Examples To enter trigger configuration mode for trigger `12` use the command:

```
awplus# trigger 12
```

To completely remove all configuration associated with trigger `12`, use the command:

```
awplus# no trigger 12
```

Related Commands **show trigger**
trigger activate

trigger activate

This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

Syntax `trigger activate <1-250>`

Parameter	Description
<1-250>	A trigger ID.

Mode Privileged Exec

Usage This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it is configured as inactive. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

Example To manually activate trigger `12` use the command:

```
awplus# trigger activate 12
```

Related Commands **show trigger**
trigger

type atmf node

This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax `type atmf node {join|leave}`

Parameter	Description
`join`	AMF node join event.
`leave`	AMF node leave event.

Mode Trigger Configuration

Caution **Only configure this trigger on one device because it is a network wide event.**

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
========

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------


==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!


============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related Commands **show trigger**

type cpu

This command configures a trigger to activate based on CPU usage level. Selecting the **up** option causes the trigger to activate when the CPU usage exceeds the specified usage level. Selecting the **down** option causes the trigger to activate when CPU usage drops below the specified usage level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax `type cpu <1-100> [up|down|any]`

Parameter	Description
<1-100>	The percentage of CPU usage at which to trigger.
`up`	Activate when CPU usage exceeds the specified level.
`down`	Activate when CPU usage drops below the specified level
`any`	Activate when CPU usage passes the specified level in either direction

Mode Trigger Configuration

Usage For an example trigger configuration that uses the **type cpu** command, see **"Capture Unusual CPU and RAM Activity" on page 75.4**.

Examples To configure trigger `28` to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger `5` to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

Related Commands **show trigger**
trigger

type interface

This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

Syntax `type interface <interface> [up|down|any]`

Parameter	Description
`<interface>`	Interface name. This can be the name of a switch port, an eth-management port, or a VLAN.
`up`	Activate when interface becomes operational.
`down`	Activate when the interface closes.
`any`	Activate when any interface link status event occurs.

Mode Trigger Configuration

Example To configure trigger `19` to be an interface trigger that activates when `port1.0.2` becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.2 up
```

Related Commands **show trigger**
trigger

type memory

This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax `type memory <1-100> [up|down|any]`

Parameter	Description
<1-100>	The percentage of memory usage at which to trigger.
`up`	Activate when memory usage exceeds the specified level.
`down`	Activate when memory usage drops below the specified level.
`any`	Activate when memory usage passes the specified level in either direction.

Mode Trigger Configuration

Examples To configure trigger `12` to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger `40` to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

Related Commands **show trigger**
trigger

type periodic

This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

Syntax `type periodic <1-1440>`

Parameter	Description
<1-1440>	The number of minutes between activations.

Mode Trigger Configuration

Usage A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

For an example trigger configuration that uses the **type periodic** command, see **"See Daily Statistics" on page 75.6**.

Example To configure trigger `44` to activate periodically at `10` minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

Related Commands **show trigger**
trigger

type ping-poll

This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

Syntax `type ping-poll <1-100> {up|down}`

Parameter	Description
<1-100>	The ping poll ID.
`up`	The trigger activates when ping polling detects that the target is reachable.
`down`	The trigger activates when ping polling detects that the target is unreachable.

Mode Trigger Configuration

Example To configure trigger `106` to activate when ping poll `12` detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

Related Commands **show trigger**
trigger

type reboot

This command configures a trigger that activates when your device is rebooted.

Syntax `type reboot`

Mode Trigger Configuration

Example To configure trigger `32` to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

Related Commands **show trigger**
trigger

type stack disabled-master

This command (configured to the stack) configures a trigger to activate on a stack member if it becomes the disabled master.

A disabled master has the same configuration as the active master, but has all its links shutdown.

Although this command could activate any trigger script, the intention here is that the script will reactivate the links from their previously shutdown state, to enable the user to manage the switch. An appropriate trigger script must already exist that will apply the **no shutdown** command on page 12.15 on the deactivated links.

Caution **It is important that any ports that are configured as trunked ports across master and stack members are disabled at their stack member termination when operating in the fallback configuration. Otherwise, the trunked ports will not function correctly on the switch that is connected downstream.**

If the **stack virtual-mac** command on page 82.25 command is enabled, the stack uses a virtual MAC address. The stack will always use this MAC address and the new elected master will still retain the originally configured virtual MAC address. If the **stack virtual-mac** command is disabled, the stack will use the MAC address of the current master. If the stack master fails, the stack MAC address changes to reflect the new master's MAC address. See **"Fixed or Virtual MAC Addressing" on page 81.13** for information on virtual MAC addresses.

Syntax

```
type stack disabled-master
```

Mode Trigger Configuration

Examples To configure trigger `82` to activate on a device if it becomes the disabled master, use the commands:

`awplus#` `configure terminal`	Enter the Global Configuration mode
`awplus(config)#` `trigger 82`	Enter the Trigger Configuration mode for trigger 82
`awplus(config-trigger)#` `type stack disabled master`	Sets the type of trigger
`awplus(config-trigger)#` `script 1 flash:/disabled.scp`	
`awplus(config-trigger)#` `exit`	

Related Commands

stack disabled-master-monitoring
trigger
type stack master-fail
type stack member
type stack link

type stack link

This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a stacking link is either activated or deactivated.

Syntax `type stack link {up|down}`

Parameter	Description
`up`	Stack link up event
`down`	Stack link down event

Mode Trigger Configuration

Example To configure trigger `86` to activate when the stack link down event occurs, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack link down
```

Related Commands
show trigger
trigger
type stack master-fail

type stack master-fail

This command (configured to the stack) initiates the action of a pre-configured trigger to occur when the stack enters the fail-over state.

Syntax `type stack master-fail`

Mode Trigger Configuration

Example To configure trigger `86` to activate when stack master fail-over event occurs, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack master-fail
```

Related Commands
stack disabled-master-monitoring
trigger
type stack disabled-master
type stack member
type stack link

type stack member

This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a switch either joins or leaves the stack.

Syntax

```
type stack member {join|leave}
```

Parameter	Description
`join`	Neighbor join event
`leave`	Neighbor leave event

Mode

Trigger Configuration

Example

To configure a pre-configured trigger number `86` to activate when a new switch joins the stack.

Note that the number `86` has no particular significance: you can assign any (previously created) numbered trigger.

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack member join
```

Related Commands

trigger
type stack master-fail
type stack link

type time

This command configures a trigger that activates at a specified time of day.

Syntax `type time <hh:mm>`

Parameter	Description
<hh:mm>	The time to activate the trigger.

Mode Trigger Configuration

Usage A combined limit of 10 triggers of the type time and type periodic can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

Example To configure trigger `86` to activate at `15:53`, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type time 15:53
```

Related Commands **show trigger**
trigger

type usb

Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.

Syntax `type usb {in|out}`

Parameter	Description
`in`	Trigger activates on insertion of a USB storage device.
`out`	Trigger activates on removal of a USB storage device.

Mode Trigger Configuration

Usage USB triggers cannot execute script files from a USB storage device.

For example trigger configurations that use the **type usb** command, see **"Capture Show Output and Save to a USB Storage Device" on page 75.11**.

Examples To configure `trigger 1` to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

Related Commands
trigger
show running-config trigger
show trigger

undebug trigger

This command applies the functionality of the **no debug trigger** command.

Chapter 77: Cable Fault Locator Introduction

Introduction to the Cable Fault Locator 77.2
Capabilities 77.2
TDR Operating Principles 77.2
Using the Cable Fault Locator 77.3

Introduction to the Cable Fault Locator

The Cable Fault Locator (CFL) is a cable diagnostic tool located within the switch. For a selected port, the CFL will display connection status or faults that exist in either the connecting cable itself, or its terminations.

Capabilities

The CFL is designed to operate on cable systems that utilize the following:

- fixed copper ports, i.e. not using SFP type pluggable transceivers.
- unshielded twisted pair data cables such as CAT 5 or CAT 6 and up to 100 meters long.
- cable terminations that use RJ-45 or RJ-0.5 connections.
- data rates from 10 Mbps to 1 Gbps (10 Gbps over copper cable is not supported).

The CFL operates using a technology known as Time Domain Reflectometry (TDR) to test all four pairs of wires inside the cable.

Note that CFL cannot run on a port that is currently supplying power via PoE.

TDR Operating Principles

When a data cable is correctly terminated, the data energy traveling along it is absorbed by its terminating load resistance. However, if the cable is unplugged, broken or short circuited, this energy is reflected at the cable termination and travels back along the cable towards its source connection.

To test the cable, the CFL generates a pulse at the cable source connection and monitors the cable for the presence of a returning (reflected) pulse. By measuring the timing between the transmitted and reflected pulses, the CFL can calculate the distance between a fault (usually at the distant termination) and cable's source connection. Also, by detecting the polarity of the reflected signal, the CFL can determine whether the fault is due to an open circuit, or a short circuit, condition.

Using the Cable Fault Locator

To run a CFL diagnostics test, use the command, **"test cable-diagnostics tdr interface" on page 78.4**. This will return a prompt asking you to confirm whether or not you want to continue with the test. This confirmation prompt is generated because the link is unable to carry data during the test, typically taking between 1 and 2 seconds to complete.

Example To run a CFL test on the cable inserted into port 1.0.1 use the following command:

```
awplus# test cable-diagnostics tdr interface
        port1.0.1
```

This command returns the following message:

```
Link will go down while test is in progress. Continue? (y/n):
```

Select y to continue.

```
awplus# y
```

Answering y returns the following message:

```
Test started. This will take several seconds to complete. Use
"show test cable-diagnostics tdr" to print results.
```

Once the cable test has run you can display its results by running the **show test cable-diagnostics tdr** command on page 78.3.

Output **Figure 77-1: Example output from the show test cable-diagnostics tdr command**

```
Port     Pair Length       Status
-----------------------------------------
1.0.1    A    -            OK
         B    -            OK
         C    5 +/- 5 m    Open
```

From the monitoring tests described, the CFL presents cable termination status information as shown, together with explanations, in **Table 77-1**.

Table 77-1: Cable status table

Status	Definition
OK	The pair is good and is terminated.
Open	The pair is not terminated.
Short (within-pair)	There is a short between the two wires of the pair.
Short (cross-pair)	There is a short between wires of different pairs.
Error	The test was unable to get a result. This error condition may occur when connecting to remote devices that issue idle traffic data when operating in the 10/100 M mode.

Chapter 78: Cable Fault Locator Commands

Command List 78.2
clear test cable-diagnostics tdr 78.2
show test cable-diagnostics tdr 78.3
test cable-diagnostics tdr interface 78.4

Command List

This chapter provides an alphabetical reference of commands used to test copper cables. For more information, see Cable Tester Introduction.

clear test cable-diagnostics tdr

This command clears the results of the last cable test that was run.

Syntax `clear test cable-diagnostics tdr`

Mode Privileged Exec

Examples To clear the results of a previous cable-diagnostics test use the following commands:

```
awplus# clear test cable-diagnostics tdr
```

show test cable-diagnostics tdr

This command displays the results of the last cable-diagnostics test that was run using the TDR (Time Domain Reflectometry) on a fixed copper cable port.

The displayed status of the cable can be either:

- OK
- Open
- Short (within-pair)
- Short (across-pair)
- Error

Syntax

```
show test cable-diagnostics tdr

no enable
```

Mode Privileged Exec

Examples To show the results of a cable-diagnostics test use the following command:

```
awplus# show test cable-diagnostics tdr
```

Output **Figure 78-1: Example output from the show test cable-diagnostics tdr command**

```
Port      Pair Length       Status
------------------------------------------
1.0.1     A    -            OK
          B    -            OK
          C    5 +/- 5 m    Open
```

test cable-diagnostics tdr interface

This command applies the Cable Fault Locator's cable-diagnostics tests to twisted pair data cables for a selected port. The tests will detect either correct, short circuit, or open, circuit terminations. For more information on running the CFL, see the **Cable Fault Locator Introduction** chapter.

The test can take several seconds to complete. See the related show command to display the test results.

A new test can only be started if no other test is in progress. CFL cannot run on a port that is currently supplying power via PoE.

The displayed status of the cable can be either, OK, Short (within-pair), or Open. The "Open" or "Short" status is accompanied with the distance from the source port to the incorrect termination.

Syntax `test cable-diagnostics tdr interface <interface>`

Parameter	Description
`cable-diagnostics`	The cable diagnostic tests.
`tdr`	Time Domain Reflectometry.
`interface`	Selects the interface to test.
`<interface>`	Interface number of the port to be tested, i.e. 1.0.2.

Example To run a cable test on the cable inserted into port 1.0.1 use the following command:

```
awplus# test cable-diagnostics tdr interface
       port1.0.1
```

You will receive the following message:

```
Link will go down while test is in progress. Continue? (y/n):
y Select y to continue.
```

```
awplus# y
```

You will then receive the following message:

```
Test started. This will take several seconds to complete. Use
"show test cable-diagnostics tdr" to print results.
```

Chapter 79: Ping Polling Introduction and Configuration

Introduction 79.2
How Ping Polling Works 79.2
Configuring Ping Polling 79.4
    Creating a Polling Instance 79.4
    Customizing a Polling Instance 79.5
    Troubleshooting Ping Polling 79.6
Interaction with Other Protocols 79.7

Introduction

Ping polling lets your device regularly check whether it can reach other hosts on a network. It works by sending ICMP Echo Requests to a host and waiting for replies sent back. If ping polling indicates that a host's status has changed, then your device can respond to the new status. When a host is unreachable, ping polling continues monitoring the host's reachability.

You can configure triggers to activate when ping polling determines that the host's status has changed. For example, you could configure a trigger to run a script that opens and configures an alternative link if the host at the other end of a preferred link becomes unavailable. You could then configure a second trigger to run a script that automatically returns traffic to the preferred link as soon as it is available again.

How Ping Polling Works

To determine a host's reachability, your device regularly sends ICMP Echo Request packets ("pings") to the host. As long as your device receives ping responses from the host, it considers the host to be reachable. If your device does not receive a reply to a set number of ICMP Echo Requests, it considers that the host is unreachable. It continues to try to ping the device, at an increased rate. After it receives a set number of responses, it considers the device to be reachable again.

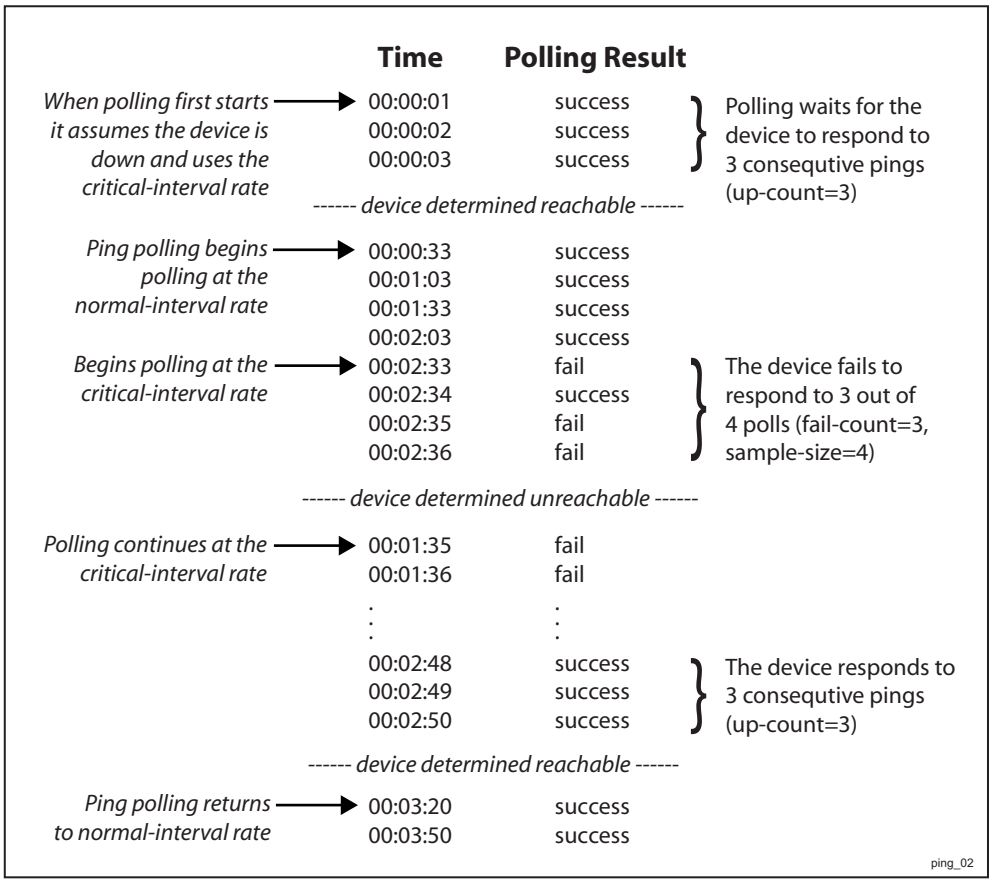
By default, a polling instance sends a ping every 30 seconds as long as it is receiving replies. The frequency of this polling is controlled by the normal-interval command. When a reply is not received, the polling instance increases the frequency at which it polls the device. This frequency is controlled by the critical-interval command, and by default, is set to send a packet every one second. It maintains this higher rate of polling until it has received sufficient consecutive replies.

The polling instance determines whether a device is reachable or unreachable based on the settings of the fail-count, sample-size, and up-count commands. To determine whether a device is reachable, the polling instance counts the number of failed pings within a set sample size. The sample size is set by the sample-size command, and by default is 5 ping responses. Within the sample size, the number of failed pings that means that the device is down is set by the fail-count command. By default this is set to 5. Once a polling instance has determined that a device is unreachable, it must receive a set number of consecutive replies before it changes the device's status back to reachable. This number is configured with the up-count command.

The following figure illustrates a polling instance where the device becomes unreachable, then reachable. It uses this configuration:

```
awplus(config-ping-poll)# fail-count 4
awplus(config-ping-poll)# sample-size 5
awplus(config-ping-poll)# up-count 3
awplus(config-ping-poll)# critical-interval 1
awplus(config-ping-poll)# normal-interval 30
```

Figure 79-1: Interaction between states and parameters for ping polling



On some operating systems, some servers may respond to a ping even if no other functionality is available, and therefore remain in an Up state while malfunctioning.

Responding to status changes

To configuring your device to determine and respond to changes in a device's reachability, you will need to:

- create a polling instance to periodically ping the device
- create scripts to run when the device becomes unreachable and when it becomes reachable again
- configure triggers to run these scripts

To set a trigger to activate when a device's status changes, its trigger type must be **ping-poll**. This is with the following command in the trigger's configuration mode:

```
awplus(config-trigger)# type ping-poll <1-100> {up|down}
```

where **up** activates the trigger when the device is reachable, and **down** activates the trigger when the device is unreachable.

If you use triggers to open a backup link to a remote device in the event of the primary link failing (rather than the remote device failing), the backup link and primary link must point to different IP addresses on the remote device. Otherwise, when the backup link points to the IP address that your device is polling, your device receives ping replies through the backup link, considers the device to be reachable again, and attempts to reopen the primary link instead of using the backup link. See **Chapter 74, Triggers Introduction** for more information about configuring Triggers with Ping Polling.

Configuring Ping Polling

This section contains:

- **Creating a Polling Instance**
  This explains how to quickly create a polling instance using the ping polling defaults.
- **Customizing a Polling Instance**
  This explains how to customize a ping poll and explains the other ping poll commands.
- **Troubleshooting Ping Polling**
  This explains how to use the debugging and monitoring commands for ping polling.

Creating a Polling Instance

The Ping Polling feature in the AlliedWare Plus™ OS allows you to easily configure polling instances with a minimum of commands. To configure a ping poll suitable for most network situations:

1. Create a polling instance by using the command:

```
awplus(config)# ping-poll <1-100>
```

   The range **<1-100>** identifies the polling instance in the trigger commands and in other ping poll commands. Your device can poll up to 100 IP addresses at once.

2. Set the IP address of the device you are polling by using the command:

```
awplus(config-ping-poll)# ip {<ip-address>|<ipv6-address>}
```

3. Enable the polling instance by using the command:

```
awplus(config-ping-poll)# active
```

4. If desired, set an optional description to identify the polling instance, by using the command:

```
awplus(config-ping-poll)# description <description>
```

You do not need to configure any other commands for most networks, because convenient defaults exist for all other ping poll settings. The following table summarizes the default configuration created.

Command	Default
Critical-interval	1 second
Fail-count	5
Length	32 bytes
Normal-interval	30 seconds

Command(cont.)	Default(cont.)
Sample-size	5
Source-ip	The IP address of the interface from which the ping packets are transmitted
Time-out	1 second
Up-count	30

Customizing a Polling Instance

Once you've created a polling instance using the ping-poll and **ip (ping-polling)** command, you may wish to customize the polling instance for your network.

Packet size

If you find that larger packet types in your network are not reaching the polled device while smaller ones such as ping do, you can increase the data bytes included in the ping packets sent by the polling instance. This encourages the polling instance to change the device's status to unreachable when packet of the size you are interested in are being dropped. To change the number of bytes sent in the data portion of the ping packets, use the command:

```
awplus(config-ping-poll)# length <4-1500>
```

Response timeout

The polling instance determines that a device hasn't responded to a ping if one second elapses without a response to the ping. In networks where ping packets have a low priority, you may need to set the allowed response time to a longer time period. To change this, use the command:

```
awplus(config-ping-poll)# timeout <1-30>
```

Polling frequency

By default, a polling instance polls a reachable device every 30 seconds. You can change this by using the command:

```
awplus(config-ping-poll)# normal-interval <1-65536>
```

Once the polling instance has determined that a ping has failed, it starts polling the device at the frequency set as the critical interval—by default, one second. To change the frequency set by the critical interval, use the command:

```
awplus(config-ping-poll)# critical-interval <1-65536>
```

The critical interval enables the polling instance to quickly observe changes in the state of the device, and should be set to a much lower value than the normal interval.

Configuring when the device's status changes

The number of pings that the polling instance examines to consider a change in state is controlled by the interaction of the sample-size, fail-count, and up-count commands. See **"How Ping Polling Works" on page 79.2** for an example showing this interaction.

To determine whether a device is reachable, the polling instance counts the number of failed pings within a sample of a set size. The sample size is 5 pings by default. To change the sample size, use the command:

```
awplus(config-ping-poll)# sample-size <1-100>
```

To change the number of failed pings that the sample must have, use the command:

```
awplus(config-ping-poll)# fail-count <1-100>
```

If the sample size and fail count are the same, the unanswered pings must be consecutive. If the sample size is greater than the fail count, a device that does not always reply to pings may be declared unreachable.

The upcount is the number of consecutive pings that must be answered for the polling instance to consider the device reachable again. To change this from the default of 30, use the command:

```
awplus(config-ping-poll)# up-count <1-100>
```

Checking the configuration

To check the settings and status of the polling instance, use the command:

```
awplus(config-ping-poll)# show ping-poll [<1-100>|state {up|
                          down}] [brief]
```

Troubleshooting Ping Polling

To disable a polling instance, use the command:

```
awplus(config-ping-poll)# no active
```

The polling instance no longer sends ICMP echo requests to the polled device and the counters for this polling instance are reset.

To clear the counters and change the status of a device to unreachable, enter the Privileged Exec mode and use the command:

```
awplus# clear ping-poll {<1-100>|all}
```

The polling instance changes to the polling frequency specified with the critical-interval command. The device status changes to reachable once the device responses have reached the **up-count**.

To start debugging for ping polling, use the command:

```
awplus# debug ping-poll <1-100>
```

Interaction with Other Protocols

Ping polling does not work if the polled host, your device, or any intermediate routers or switches are configured to drop ICMP Echo Requests and Replies.

Ping and Traceroute

Ping and Traceroute are not affected by ping polling. You can enter ping and trace commands at any time and independent of the polling.

Chapter 80: Ping-Polling Commands

Command List 80.2
active (ping-polling) 80.3
clear ping-poll 80.4
critical-interval 80.5
debug ping-poll 80.6
description (ping-polling) 80.7
fail-count 80.8
ip (ping-polling) 80.9
length (ping-poll data) 80.10
normal-interval 80.11
ping-poll 80.12
sample-size 80.13
show counter ping-poll 80.14
show ping-poll 80.16
source-ip 80.20
timeout (ping polling) 80.21
up-count 80.22
undebug ping-poll 80.22

Command List

This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see **Chapter 79, Ping Polling Introduction and Configuration**.

For information about modifying or redirecting the output from **show** commands to a file, see **"Controlling "show" Command Output" on page 1.35**.

Table 80-1: The following table lists the default values when configuring a ping poll

Default	Value
Critical-interval	1 second
Description	No description
Fail-count	5
Length	32 bytes
Normal-interval	30 seconds
Sample-size	5
Source-ip	The IP address of the interface from which the ping packets are transmitted
Time-out	1 second
Up-count	30

active (ping-polling)

This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the **ip (ping-polling)** command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

Syntax

```
active
no active
```

Mode Ping-Polling Configuration

Examples To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

Related Commands

debug ping-poll
ip (ping-polling)
ping-poll
show ping-poll

clear ping-poll

This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the **critical-interval** command. The device status changes to reachable once the device responses have reached the **up-count**.

Syntax `clear ping-poll {<1-100>|all}`

Parameter	Description
`<1-100>`	A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable.
`all`	Clears the counters and changes the device status of all polling instances.

Mode Privileged Exec

Examples To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

Related Commands
active (ping-polling)
ping-poll
show ping-poll

critical-interval

This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the **normal-interval** command.

The **no** variant of this command sets the critical interval to the default of one second.

Syntax

```
critical-interval <1-65536>
no critical-interval
```

Parameter	Description
<1-65536>	Time in seconds between pings, when the device has failed to a ping, or the device is unreachable.

Default The default is 1 second.

Mode Ping-Polling Configuration

Examples To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

Related Commands

fail-count
normal-interval
sample-size
show ping-poll
timeout (ping polling)
up-count

debug ping-poll

This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

Syntax

```
debug ping-poll <1-100>
no debug ping-poll {<1-100>|all}
```

Parameter	Description
<1-100>	A unique ping poll ID number.
all	Turn off all ping-poll debugging.

Mode Privileged Exec

Examples To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

Related Commands

active (ping-polling)
clear ping-poll
ping-poll
show ping-poll
undebug ping-poll

description (ping-polling)

This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	The description of the target. Valid characters are any printable character and spaces. There is no maximum character length.

Mode Ping-Polling Configuration

Examples To add the text “Primary Gateway” to describe the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# description Primary Gateway
```

To delete the description set for the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no description
```

Related Commands **ping-poll**
show ping-poll

fail-count

This command specifies the number of pings that must be unanswered, within the total number of pings specified by the **sample-size** command, for the ping-polling instance to consider the device unreachable.

If the number set by the **sample-size** command and the **fail-count** commands are the same, then the unanswered pings must be consecutive. If the number set by the **sample-size** command is greater than the number set by the **fail-count** command, then a device that does not always reply to pings may be declared unreachable.

The **no** variant of this command resets the fail count to the default.

Syntax

```
fail-count <1-100>
no fail-count
```

Parameter	Description
<1-100>	The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable.

Default The default is 5.

Mode Ping-Polling Configuration

Examples To specify the number of pings that must fail within the sample size to determine that a device is unreachable for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# fail-count 5
```

To reset the fail-count to its default of 5 for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no fail-count
```

Related Commands

critical-interval
normal-interval
ping-poll
sample-size
show ping-poll
timeout (ping polling)
up-count

ip (ping-polling)

This command specifies the IPv4 address of the device you are polling.

Syntax `ip {<ip-address>|<ipv6-address>}`

Parameter	Description
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	An IPv6 address in hexadecimal notation `X:X::X:X`

Mode Ping-Polling Configuration

Examples To set ping-poll instance 5 to poll the device with the IP address `192.168.0.1`, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 5
awplus(config-ping-poll)# ip 192.168.0.1
```

To set ping-poll instance 10 to poll the device with the IPv6 address `2001:db8::`, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 10
awplus(config-ping-poll)# ip 2001:db8::
```

Related Commands
ping-poll
source-ip
show ping-poll

length (ping-poll data)

This command specifies the number of data bytes to include in the data portion of the ping packet. This allows you to set the ping packets to a larger size if you find that larger packet types in your network are not reaching the polled device, while smaller packets are getting through. This encourages the polling instance to change the device's status to unreachable when the network is dropping packets of the size you are interested in.

The **no** variant of this command resets the data bytes to the default of 32 bytes.

Syntax

```
length <4-1500>
no length
```

Parameter	Description
<4-1500>	The number of data bytes to include in the data portion of the ping packet.

Default The default is 32.

Mode Ping-Polling Configuration

Examples To specify that ping-poll instance 12 sends ping packet with a data portion of 56 bytes, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length 56
```

To reset the number of data bytes in the ping packet to the default of 32 bytes for ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length
```

Related Commands **ping-poll**
show ping-poll

normal-interval

This command specifies the time period between pings when the device is reachable.

The **no** variant of this command resets the time period to the default of 30 seconds.

Syntax

```
normal-interval <1-65536>
no normal-interval
```

Parameter	Description
<1-65536>	Time in seconds between pings when the target is reachable.

Default The default is 30 seconds.

Mode Ping-Polling Configuration

Examples To specify a time period of 60 seconds between pings when the device is reachable for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# normal-interval 60
```

To reset the interval to the default of 30 seconds for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no normal-interval
```

Related Commands

critical-interval
fail-count
ping-poll
sample-size
show ping-poll
timeout (ping polling)
up-count

ping-poll

This command enters the ping-poll configuration mode. If a ping-poll exists with the specified number, then this command enters its configuration mode. If no-ping poll exists with the specified number, then this command creates a new ping poll with this ID number.

To configure a ping-poll, create a ping poll using this command, and use the **ip (ping-polling)** command to specify the device you want the polling instance to poll. It is not necessary to specify any further commands unless you want to change a command's default.

The **no** variant of this command deletes the specified ping poll.

Syntax

```
ping-poll <1-100>
no ping-poll <1-100>
```

Parameter	Description
<1-100>	A unique ping poll ID number.

Mode Global Configuration

Examples To create ping-poll instance 3 and enter ping-poll configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 3
awplus(config-ping-poll)#
```

To delete ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# no ping-poll 3
```

Related Commands

active (ping-polling)
clear ping-poll
debug ping-poll
description (ping-polling)
ip (ping-polling)
length (ping-poll data)
show ping-poll
source-ip

sample-size

This command sets the total number of pings that the polling instance inspects when determining whether a device is unreachable. If the number of pings specified by the **fail-count** command go unanswered within the inspected sample, then the device is declared unreachable.

If the numbers set in this command and **fail-count** command are the same, the unanswered pings must be consecutive. If the number set by this command is greater than that set with the **fail-count** command, a device that does not always reply to pings may be declared unreachable.

You cannot set this command's value lower than the **fail-count** value.

The polling instance uses the number of pings specified by the **up-count** command to determine when a device is reachable.

The **no** variant of this command resets this command to the default.

Syntax

```
sample-size <1-100>
no sample size
```

Parameter	Description
<1-100>	Number of pings that determines critical and up counts.

Default The default is 5.

Mode Ping-Polling Configuration

Examples To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```

Related Commands

critical-interval
fail-count
normal-interval
ping-poll
show ping-poll
timeout (ping polling)
up-count

show counter ping-poll

This command displays the counters for ping polling.

Syntax `show counter ping-poll [<1-100>]`

Parameter	Description
<1-100>	A unique ping poll ID number. This displays the counters for the specified ping poll only. If you do not specify a ping poll, then this command displays counters for all ping polls.

Mode User Exec and Privileged Exec

Output **Figure 80-1: Example output from the show counter ping-poll command**

```
Ping-polling counters
Ping-poll: 1
PingsSent               ......... 15
PingsFailedUpState      ......... 0
PingsFailedDownState    ......... 0
ErrorSendingPing        ......... 2
CurrentUpCount          ......... 13
CurrentFailCount        ......... 0
UpStateEntered          ......... 0
DownStateEntered        ......... 0

Ping-poll: 2
PingsSent               ......... 15
PingsFailedUpState      ......... 0
PingsFailedDownState    ......... 0
ErrorSendingPing        ......... 2
CurrentUpCount          ......... 13
CurrentFailCount        ......... 0
UpStateEntered          ......... 0
DownStateEntered        ......... 0

Ping-poll: 5
PingsSent               ......... 13
PingsFailedUpState      ......... 0
PingsFailedDownState    ......... 2
ErrorSendingPing        ......... 2
CurrentUpCount          ......... 9
CurrentFailCount        ......... 0
UpStateEntered          ......... 0
DownStateEntered        ......... 0
```

Table 80-2: Parameters in output of the show counter ping-poll command

Parameter	Description
`Ping-poll`	The ID number of the polling instance.
`PingsSent`	The total number of pings generated by the polling instance.
`PingsFailedUpState`	The number of unanswered pings while the target device is in the Up state. This is a cumulative counter for multiple occurrences of the Up state.

Table 80-2: Parameters in output of the show counter ping-poll command(cont.)

Parameter	Description
`PingsFailedDownState`	Number of unanswered pings while the target device is in the Down state. This is a cumulative counter for multiple occurrences of the Down state.
`ErrorSendingPing`	The number of pings that were not successfully sent to the target device. This error can occur when your device does not have a route to the destination.
`CurrentUpCount`	The current number of sequential ping replies.
`CurrentFailCount`	The number of ping requests that have not received a ping reply in the current sample-size window.
`UpStateEntered`	Number of times the target device has entered the Up state.
`DownStateEntered`	Number of times the target device has entered the Down state.

Example To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

Related Commands
debug ping-poll
ping-poll
show ping-poll

show ping-poll

This command displays the settings and status of ping polls.

Syntax `show ping-poll [<1-100>|state {up|down}] [brief]`

Parameter	Description	
<1-100>	Displays settings and status for the specified polling instance.	
`state`	Displays polling instances based on whether the device they are polling is currently reachable or unreachable.	
	`up`	Displays polling instance where the device state is reachable.
	`down`	Displays polling instances where the device state is unreachable.
`brief`	Displays a summary of the state of ping polls, and the devices they are polling.	

Mode User Exec and Privileged Exec

Output **Figure 80-2: Example output from the show ping-poll brief command**

```
Ping Poll Configuration
-------------------------------------------------------
Id Enabled State Destination
-------------------------------------------------------
1  Yes     Down  192.168.0.1
2  Yes     Up    192.168.0.100
```

Table 80-3: Parameters in output of the show ping-poll brief command

Parameter	Meaning	
Id	The ID number of the polling instance, set when creating the polling instance with the **ping-poll** command.	
Enabled	Whether the polling instance is enabled or disabled.	
`State`	The current status of the device being polled:	
	`Up`	The device is reachable.
	`Down`	The device is unreachable.
	`Critical Up`	The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.
	`Critical Down`	The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.

Table 80-3: Parameters in output of the show ping-poll brief command(cont.)

Parameter	Meaning
Destination	The IP address of the polled device, set with the **ip (ping-polling)** command.

Figure 80-3: Example output from the show ping-poll command

```
Ping Poll Configuration
---------------------------------------------------------

Poll 1:
Description                         : Primary Gateway
Destination IP address              : 192.168.0.1
Status                              : Down
Enabled                             : Yes
Source IP address                   : 192.168.0.10
Critical interval                   : 1
Normal interval                     : 30
Fail count                          : 10
Up count                            : 5
Sample size                         : 50
Length                              : 32
Timeout                             : 1
Debugging                           : Enabled


Poll 2:
Description                         : Secondary Gateway
Destination IP address              : 192.168.0.100
Status                              : Up
Enabled                             : Yes
Source IP address                   : Default
Critical interval                   : 5
Normal interval                     : 60
Fail count                          : 20
Up count                            : 30
Sample size                         : 100
Length                              : 56
Timeout                             : 2
Debugging                           : Enabled
```

Table 80-4: Parameters in output of the show ping-poll command

Parameter	Description
Description	Optional description set for the polling instance with the **description (ping-polling)** command.
Destination IP address	The IP address of the polled device, set with the **ip (ping-polling)** command.

Table 80-4: Parameters in output of the show ping-poll command(cont.)

Parameter	Description	
`Status`	The current status of the device being polled:	
	`Up`	The device is reachable.
	`Down`	The device is unreachable.
	`Critical Up`	The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.
	`Critical Down`	The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.
`Enabled`	Whether the polling instance is enabled or disabled. The **active (ping-polling)** and **no active** commands enable and disable a polling instance.	
`Source IP address`	The source IP address sent in the ping packets. This is set using the **source-ip** command.	
`Critical interval`	The time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable. This is set with the **critical-interval** command.	
`Normal interval`	The time period between pings when the device is reachable. This is set with the **normal-interval** command.	
`Fail count`	The number of pings that must be unanswered, within the total number of pings specified by the **sample-size** command, for the polling instance to consider the device unreachable. This is set using the **fail-count** command.	
`Up count`	The number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again. This is set using the **up-count** command.	
`Sample size`	The total number of pings that the polling instance inspects when determining whether a device is unreachable. This is set using the **sample-size** command.	
`Length`	The number of data bytes to include in the data portion of the ping packet. This is set using the **length (ping-poll data)** command.	
`Timeout`	The time in seconds that the polling instance waits for a response to a ping packet. This is set using the **timeout (ping polling)** command.	
`Debugging`	Indicates whether ping polling debugging is **Enabled** or **Disabled**. This is set using the **debug ping-poll** command.	

Examples To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll 6 state down brief
```

Related Commands **debug ping-poll**
ping-poll

source-ip

This command specifies the source IP address to use in ping packets.

By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device's local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used.

The **no** variant of this command resets the source IP in the packets to the device's local interface IP address.

Syntax

```
source-ip {<ip-address>|<ipv6-address>}
no source-ip
```

Parameter	Description
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	An IPv6 address in hexadecimal notation `X:X::X:X`

Mode Ping-Polling Configuration

Examples To configure the ping-polling instance 43 to use the source IP address `192.168.0.1` in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 192.168.0.1
```

To configure the ping-polling instance 43 to use the source IPv6 address `2001:db8::` in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 2001:db8::
```

To reset the source IP address to the device's local interface IP address for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no source-ip
```

Related Commands

description (ping-polling)
ip (ping-polling)
length (ping-poll data)
ping-poll
show ping-poll

timeout (ping polling)

This command specifies the time in seconds that the polling instance waits for a response to a ping packet. You may find a higher time-out useful in networks where ping packets have a low priority.

The **no** variant of this command resets the set time out to the default of one second.

Syntax

```
timeout <1-30>
no timeout
```

Parameter	Description
<1-30>	Length of time, in seconds, that the polling instance waits for a response from the polled device.

Default The default is 1 second.

Mode Ping-Polling Configuration

Examples To specify the timeout as 5 seconds for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# timeout 5
```

To reset the timeout to its default of 1 second for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no timeout
```

Related Commands

critical-interval
fail-count
normal-interval
ping-poll
sample-size
show ping-poll
up-count

up-count

This command sets the number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again.

The **no** variant of this command resets the up count to the default of 30.

Syntax

```
up-count <1-100>
no up-count
```

Parameter	Description
<1-100>	Number of replied pings before an unreachable device is classified as reachable.

Default The default is 30.

Mode Ping-Polling Configuration

Examples To set the upcount to 5 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# up-count 5
```

To reset the upcount to the default value of 30 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no up-count
```

Related Commands

critical-interval
fail-count
normal-interval
ping-poll
sample-size
show ping-poll
timeout (ping polling)

undebug ping-poll

This command applies the functionality of the **no debug ping-poll** command on page 80.6.

Part 8: Virtual Chassis Stacking

- Chapter 81 VCStack Introduction
- Chapter 82 Stacking Commands

Chapter 81: VCStack Introduction

VCStack Introduction 81.2
Features of Virtual Chassis Stacking 81.2
VCStack Capable Switches 81.3
The Physical Stack 81.3
Two-Switch Stack Configuration 81.4
Multiple Switch Stack Configuration 81.4
Resilient Stacked Topology 81.5
Stack Formation 81.9
The Role of the Stack Master 81.9
Stack Management VLAN 81.10
Stack Member Failure and Recovery 81.13
Fixed or Virtual MAC Addressing 81.13
Stack Resiliency Link 81.14
Stack Failure Recovery 81.15
Stack Separation and Recovery 81.16
Stack Maintenance 81.16
Disabled Master Monitoring (DMM) 81.18
Provisioning (Stack Members) 81.20
Provisioned Board Classes 81.20
Applying Hardware Provisioning 81.20
Removing Hardware Provisioning 81.22
Displaying Provisioned Configurations 81.23
Provisioning and Configuration Management 81.24
Software Version Auto Synchronization 81.25
Introduction 81.25
How Auto Synchronization Works 81.25

VCStack Introduction

This chapter describes Virtual Chassis Stacking (VCStack), its features, and basic connection examples. For detailed descriptions of the commands used to configure VCStack, see **Chapter 82, Stacking Commands**. Also, see **Allied Telesis Support Documentation** for detailed instructions on how to install this feature.

VCStack is a group of physically separate switches that are configured to operate as a single logical switch. In order to function as a VCStack, its component switches are connected using high-speed stacking links.

Features of Virtual Chassis Stacking

Creating a VCStack greatly eases network management, because you can configure all the stacked devices via a single IP address. Creating a VCStack will often eliminate your need to configure protocols such as VRRP and Spanning Tree. VCStack also enables you to create highly resilient networks. This resiliency can be applied in several ways.

Within the stack itself, switch interconnection is via two links. The second link is able to provide an alternative data path, thus the stack will continue to function if a single switch fails. Degraded performance might occur however, due to the reduced VCStack bandwidth.

User ports can also be made extremely resilient by utilizing link aggregation. Aggregated links can span ports, modules, and even switches within the stack. Creating aggregated links that span multiple switches within a stack creates an extremely resilient configuration. Communication will still exist even if a switch and its aggregated ports fail. Refer to **Figure 81-4 on page 81.6.**

Caution

Stack operation is only supported if stack virtual-mac is enabled. For more information refer to: "Enabling the stack virtual-mac" on page 81.13 and "stack virtual-mac" on page 82.25

VCStack Capable Switches

VCStack is supported on the following Allied Telesis switch types:

- SwitchBlade® x8100 Series (VCStack Plus)
- x900-24XT, x900-24XS, x900-24XT-N
- x900-12XT/s
- SwitchBlade® x908
- DC2552XS
- x610 Series
- x510 Series
- IX5-28GPX
- x310 Series
- GS900MX/MPX Series

Note You can only create VCStacks using switches from within the same product group, for example all x610 Series switches.

Stacking connectivity and functionality varies slightly between switch types.Your GS900MX/MPX Series switch can support a maximum of four devices per stack. Consult the appropriate software reference for stacking functionality of other Allied Telesis switches.

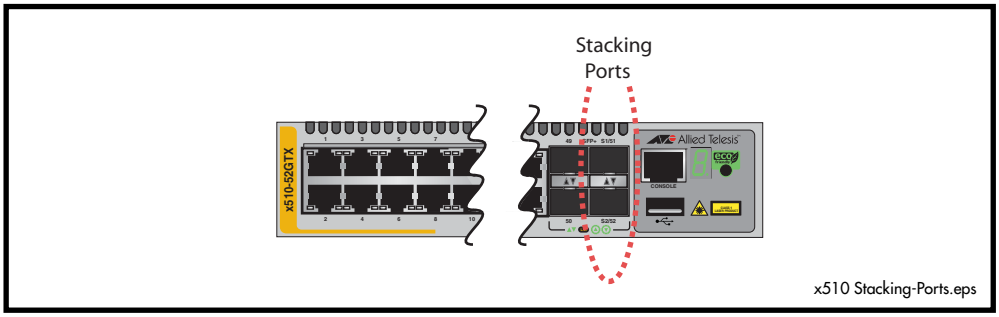
The Physical Stack

A VCStack can consist of up to four individual stack members interconnected via high-speed stacking links (SFP+ ports 25 and 26, or 49 and 50). As the stack forms, its switch members elect one of them to become the primary stack member called the stack master (displayed in the show commands as the active master). The remaining switches then become ordinary members of the stack, and are referred to as backup members.

VCStack cables and connections

Stack members are interconnected via the SFP+ ports shown in **Figure 81-1**. Note that stacking cables should connect from port 49 on one stack member, to port 50 on the other (or from port 25 on one stack member, to port 26 on the other).

Figure 81-1: Stacking ports

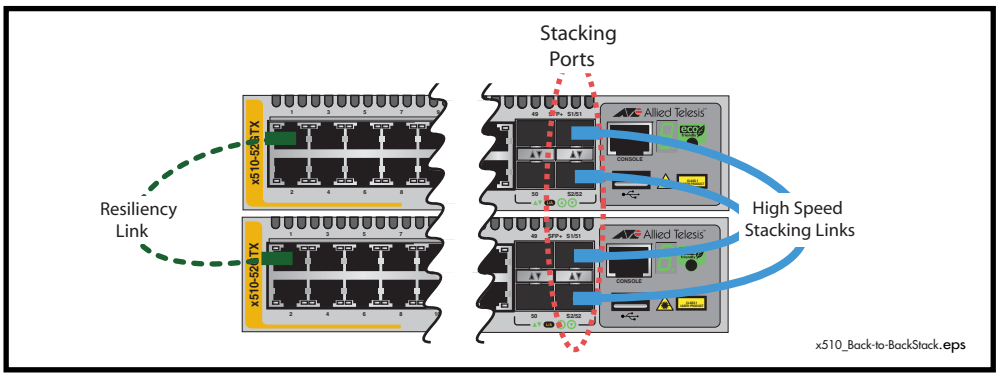


Two-Switch Stack Configuration

Ring configuration using two switches

This configuration, shown in **Figure 81-2**, uses two switches that are connected back to back via two high-speed stacking links. Note that stacking port 25 must connect to stacking port 26. Although in this configuration the stack can still function using only a single high-speed stacking link, we recommend using both stacking links as shown.

Figure 81-2: Back-to-back topology

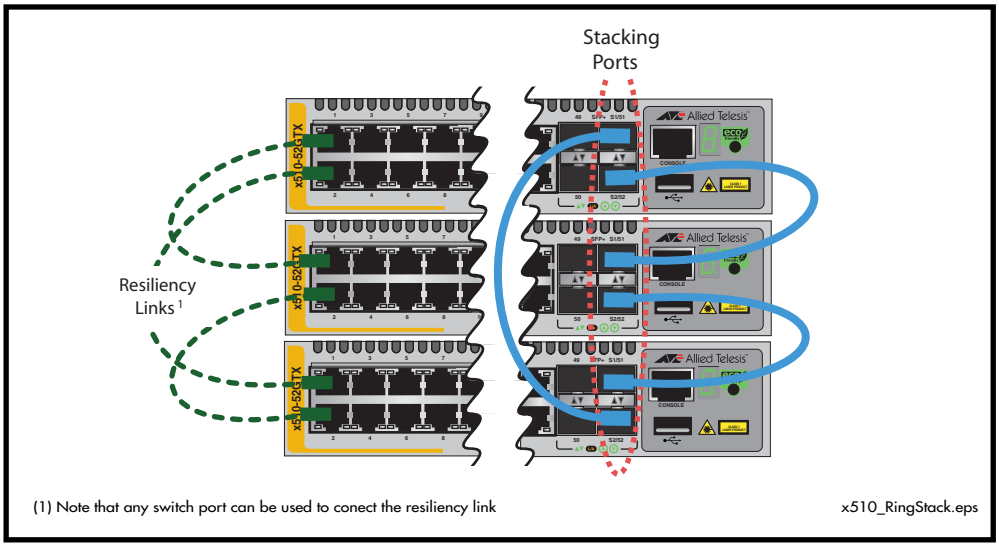


Multiple Switch Stack Configuration

Ring configuration using multiple switches

A VCStack using GS900MX/MPX series switches can comprise up to four stack members connected in a ring topology. **Figure 81-3** shows a ring comprising three stacked switches. Because alternate paths are provided between the stack members' stacking links, this topology offers a very resilient configuration.

Figure 81-3: VCStack ring topology using GS900MX/MPX series switches

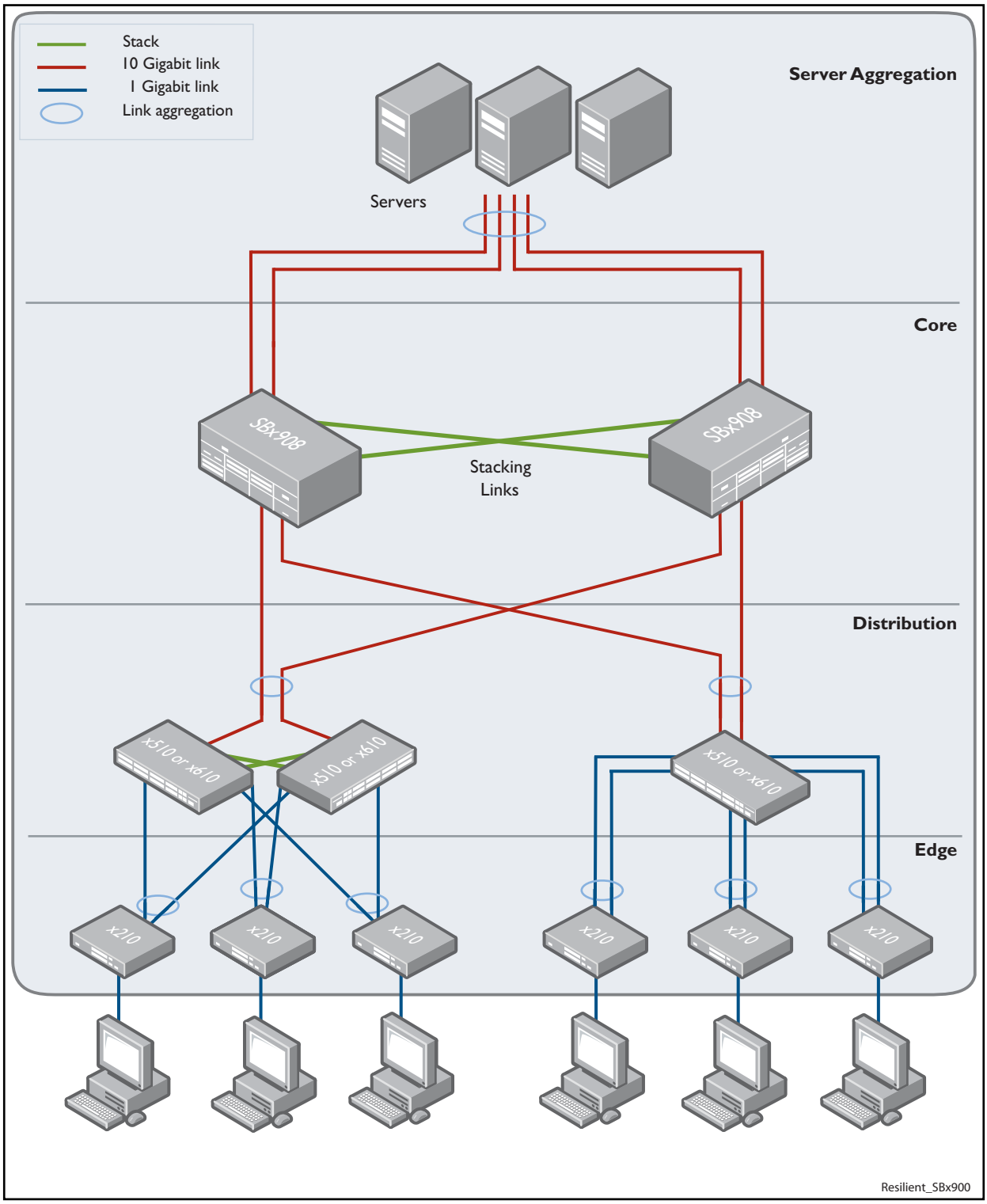


Resilient Stacked Topology

Where network connectivity uptime is a major criteria, you can use virtual chassis stacking to create highly reliable network configurations. The network shown in **Figure 81-4** employs redundant links and switches to create a stacked network that offers extremely reliable user connectivity.

Employing link aggregation rather than spanning tree to manage the parallel paths enables the bandwidth of both data links to be utilized under normal conditions, whilst enabling a single data link to operate should its partner link fail.

Figure 81-4: VCStack resilient stacked topology example



The network depicted in the above figure employs two SwitchBlade® x908 switches to form an expandable network core. These switches are stacked and so appear as a single logical switch (note that smaller switches such as can be also be used to form the stacked core or stacked distribution).

This network topology supplies multiple dual connections to a number of downstream distribution switches that can in turn connect to user devices. Similarly, the dual network paths provide very reliable connectivity to the servers portion of the network.

Resiliency link

The resiliency link carries no network data. Its function is to provide additional stack status information to enable the stack members to more accurately decide whether it is appropriate for one of them to take over the role of stack master if the existing master fails. See **"Stack Resiliency Link" on page 81.14**.

Resiliency link configurations via switch ports

Two resiliency-link configurations that use switch ports are shown below. The first figure shows the resiliency link connecting in a ring topology, whilst the second figure shows the resiliency link connecting to the switch ports via a network hub. In both configurations, the resiliency link connections are made using a designated VLAN running over switch-port connections between each stack member. For more information on using the resiliency link commands see the **stack resiliencylink** command on page 82.22 and the **switchport resiliencylink** command on page 82.27.

Figure 81-5: Resiliency link connecting to switch ports over the ResiliencyLink VLAN

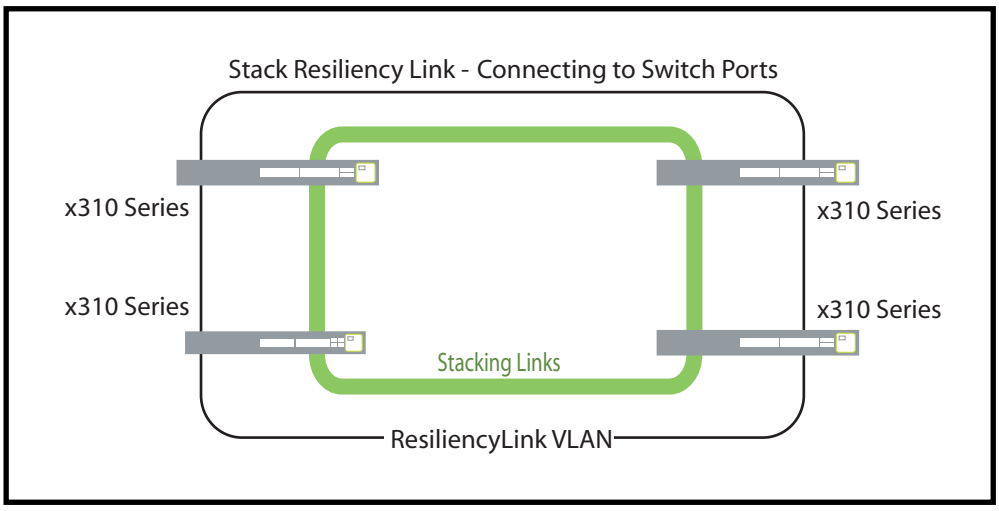
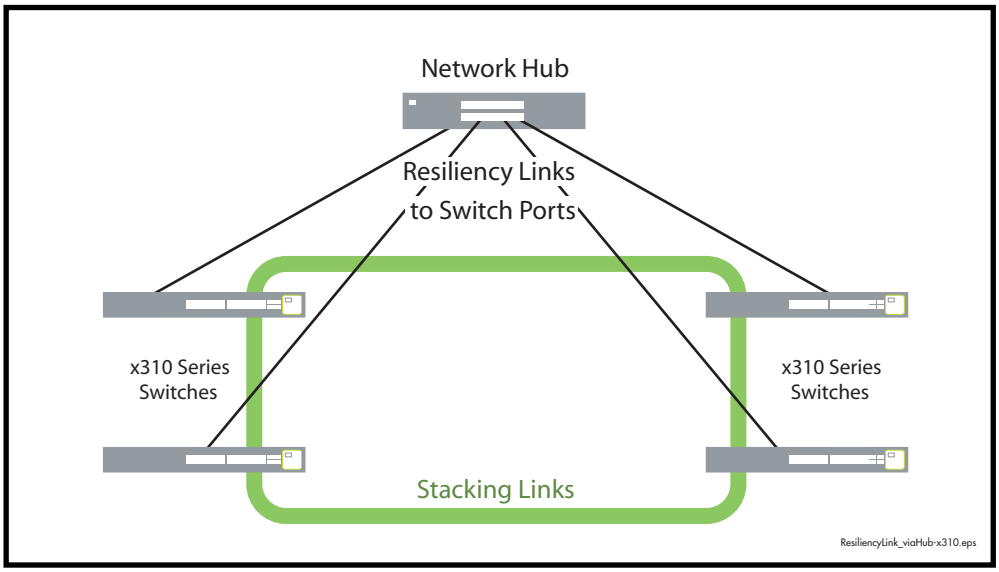


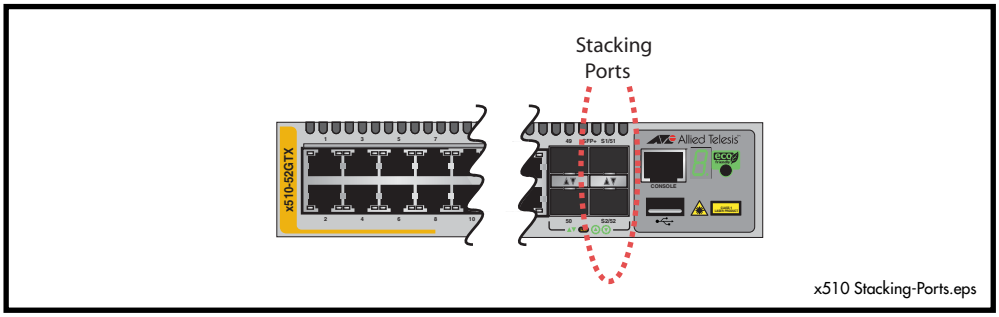
Figure 81-6: Resiliency link connecting to switch ports over the ResiliencyLink VLAN using a network hub



Stack Formation

As previously mentioned, a VCStack always contains a stack (active) master plus a number of stack (backup) members. To be part of a stack, a switch must connect to the other potential stack members via dedicated stacking ports. See **Figure 81-7**.

Figure 81-7: Stacking ports



Once the switches have been physically connected to form a stack, powering all the members on automatically sets off a number of processes that enable the stack members to detect the presence of the other stack members and form themselves into a VCStack.

The Role of the Stack Master

In addition to being a member of its VCStack, the stack master manages functions such as software version control and distribution, routing processing, and network management.

Selecting the stack master

The stack members are able to automatically select which switch will become the stack master. This selection is based on two components:

1. The stack member's priority setting.
2. The stack member's MAC address.

For both components, the lower the number the higher the priority will be. To set the stack priority, run the **stack priority** command on page 82.19. Note that changes to these settings will not take effect until the next master re-election. To display these components run the **show stack** command on page 82.11.

The master is the switch with the lowest priority setting, or if the priority settings are equal, the switch with the lowest MAC address will become the stack master. When a stack member is initially booted, its priority value defaults to 128. Therefore, if all switches retain their defaults, then the stack master will be determined by MAC address comparison.

The stack also assigns a stack-ID number to each member. This number provides a unique reference number for switches within the stack; it plays no part in selecting the stack master. The stack-ID is used as the first digit of the three component port identifier numbers. For example, port number 2.0.14 has the stack-ID of 2.

Note

This last point is an important one to remember when using configuration scripts. You should ensure that you modify your configuration scripts to match any changes you have made to the stack-ID assignments.

Note

The ability to independently set both a stack member's priority and its ID means that the stack master does not need to have an ID of 1, although configuration is simplified by arranging for ID 1 to be the device with the lowest priority value - and thereby forcing it to be the stack master. If you create a stack using new switches, the following (simplified) process should ensure that the master member has an ID of 1.

New switches are shipped with a Stack Member-ID of 1 and a priority of 128. If four such switches are created as a stack, the switch with the lowest MAC address will be selected to be the stack master (because all priority settings are 128). The remaining three stack member devices will then reboot. The stack master does not reboot and retains its Stack Member-ID of 1.

You can change the stack-ID by using the **stack renumber** command on page 82.20.

Common stack configuration

Once the switches have configured themselves into a VCStack, they all share the same configuration information and startup scripts.

Stack Management VLAN

Managing the stack is the same as managing an individual switch. You can connect to the asynchronous console port of any stack member, or you can set an IP address on a network VLAN (for example, VLAN 1) and use SSH for remote access.

As the switches form themselves into a stack, each switch creates a common stack management VLAN and a management IP address. Both the VLAN ID and the IP address are internal entities that are used between the stacked switches, via the stacking ports, and therefore do not appear on the user network.

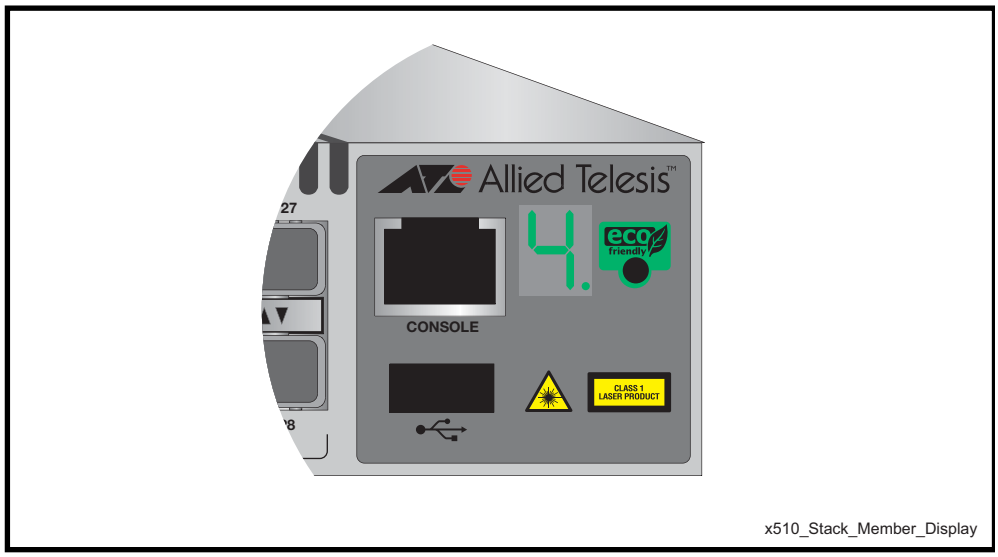
Initially the stack assigns the default VLAN tag ID of 4094 to the management VLAN, and assigns an IP address from the subnet 192.168.255.0/27 to this VLAN as the management IP address. Once the stack has formed, you can change both these settings. To change the VLAN ID use the **stack management vlan command on page 82.18**. To change the management IP address use the **stack management subnet command on page 82.17**. Note however, that you must keep the 27 bit subnet mask, (/27 or 255.255.255.224).

Also note that the management VLAN ID and management IP subnet must be unique across the stack's internal and external network. This means you cannot use the management VLAN ID or management IP subnet elsewhere in the user network. However, note that stacks in the same network can all use the same management VLAN ID and management IP subnet settings internally. To view the current settings for the stack management VLAN ID and IP address, use the **show stack command on page 82.11**.

Stack member identification

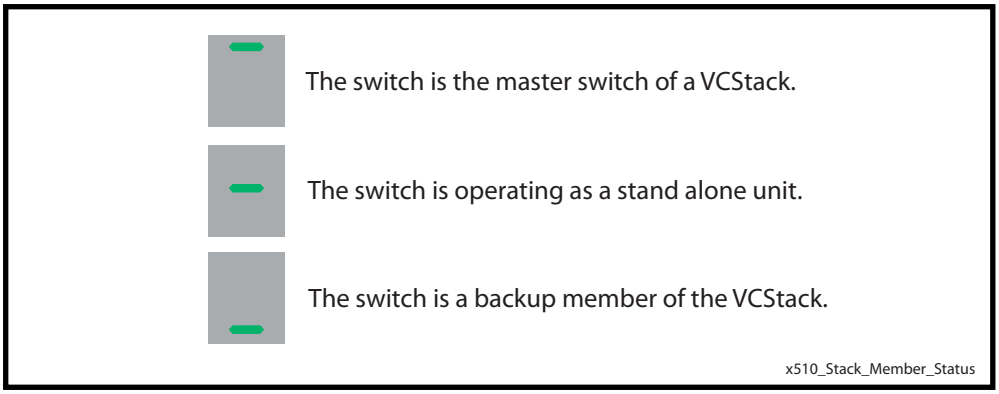
When a switch becomes a stack member, it is assigned a Stack Member ID. A numeric ID LED on the front panel indicates its stack member ID number. See **Figure 81-8 on page 81.11**. Switches in a VCStack usually have stack IDs in the range 1 to 4 (although any four numbers between 1 and 8 can be assigned). A stand-alone switch displays the ID number 0.

Figure 81-8: Stack member ID display



In addition, depressing the “eco” button on this panel will change the LED display to indicate the status of the switch within a stack, or whether it is operating as a stand alone switch. See **Figure 81-8 on page 81.11**.

Figure 81-9: Stack_Member_Status display



Running commands on specific stack members

In some situations, you may want to obtain information that is specific to a particular stack member. For many **show** commands, you can specify the desired stack member. For example, to show the processes for stack member 2, use the following command:

```
awplus# show process 2
```

In other cases, you can use the **remote-login** command to log into the specific stack member. For example, to see a directory listing for stack member 2, use the following commands:

```
awplus# remote-login 2
awplus-2# enable
awplus-2# dir
```

To return to the command prompt on the master stack member, type **exit**.

For more information on using this command, see the **remote-login command on page 82.5**.

Running QoS within a VCStack

When you configure QoS on a VCStack, you need to make the following changes:

Switches within a VCStack exchange their stack management traffic and user data over their high speed stacking links. The stack management traffic is pre-assigned to the egress queue 7. This is the highest value queue, and (in a stacked configuration) its traffic should not be shared with any user data. However, any CoS tagging of 7 applied to the incoming data will automatically be assigned to queue 7. You will therefore need to reconfigure your CoS to Queue settings to ensure that no user data is sent to queue 7.

To prevent this from happening, we recommend that you make appropriate changes to your queue settings (mappings) to reflect the stacking requirement previously described. For more information on this topic, see **"Mapping CoS tags to traffic types" on page 40.12**.

This process should include (but not be limited to) running the following command to ensure that any remaining user packets still carrying a CoS 7 tag will be mapped to egress queue 6.

To remap priority CoS traffic to egress queue 6, run the following commands:

```
awplus# config terminal
awplus(config)# mls qos map cos-queue 7 to 6
```

Stack Member Failure and Recovery

Fixed or Virtual MAC Addressing

A VCStack operates using a single virtual MAC address. This address is configurable by using the **stack virtual-mac** command on page 82.25.

Enabling the stack virtual-mac

When the **stack virtual-mac** command is enabled, the stack uses a virtual MAC address selected from an allocated pool of MAC addresses. The stack will then always use this MAC address even if the stack master fails or is removed from the stack. In this situation, the new elected master will still retain the originally configured virtual MAC address.

The virtual MAC address will be used for all external ports, and VLAN interfaces, except the management VLAN. Although each individual switch in the stack retains its own native MAC address; this is only used over the stack management VLAN.

Note

If one stack member has the virtual MAC address feature enabled and another has the virtual MAC address feature disabled then they will be able to form together as a stack. From master election onwards, the stack master's virtual MAC address setting will be used by the rest of the stack.

Caution **Stack operation is only supported if stack virtual-mac is enabled.**

Virtual MAC format and value

The virtual MAC address is selected from within the range 0000.cd37.0000 to 0000.cd37.0FFF.

This can be considered as a MAC prefix component of 0000.cd37.0xxx.

where xxx is called the stack virtual-chassis-ID, and has the range 000 to FFF.

By default, the virtual-chassis-ID is randomly selected from the available range.

To change the virtual MAC address, use the **stack virtual-chassis-id command on page 82.24**.

Note

Using the same virtual MAC address settings on stacks in the same network will result in duplicate MAC addresses and network disruption.
Please ensure each stack in your network uses a unique virtual-chassis-ID.

Manually selected virtual address

To manually select a virtual MAC address you enable the stack virtual MAC feature by using the commands:

```
awplus# configure terminal
awplus(config)# stack virtual-mac
```

Then configure the **stack virtual-chassis-id** command on page 82.24 to set a stack virtual-chassis-ID of your chosen value - entered as a decimal number within the range 0 to 4095. The value 120 is used in the following example:

```
awplus# configure terminal
awplus(config)# stack virtual-chassis-id 120
```

Automatically selected virtual address

If you set the **stack virtual-mac** command without entering a value for the stack virtual-chassis-ID, the switch will randomly select a virtual-chassis-ID from the allocated range.

Disabling the stack virtual-mac

When the **stack virtual-mac** command is disabled, the stack will use the MAC address of the current Master. If the stack master fails, the stack MAC address changes to reflect the new master's MAC address. If the stack MAC address does change, ARP tables of devices on the network will update to reflect the change in MAC address via **ip gratuitous-arp-link** command on page 25.16.

Stack Resiliency Link

The purpose of the resiliency link is to provide the stack members with status information that allows them to detect whether the stack master is still operational after a stack failure occurs.

Using the resiliency link, a stack member can differentiate between the master suffering a power-down or a software lock-up, where the master is offline, compared with a stacking-link failure, where the master is still online but connectivity over the stacking cables has been lost.

This enables the other stack members to either operate in the fall-back Disabled Master mode, or to re-elect a new stack master. The **"State change table" on page 81.14** shows how the stack members respond to various problems occurring on the master node.

Stack recovery states

The following state-change-table shows stack member failure conditions and recovery actions in situations where the resiliency link is present or absent.

Table 81-1: State change table

Event on Master Node	Reaction on Master	Reaction on Stack Member with resiliency link	Reaction on Stack Member without resiliency link
Both stack links removed	No change	**Disabled master**	Re-elect master [2]
Hardware reset (or fault)	Reset / offline	Re-elect master	Re-elect master [2]
Run the **no stack enable** command[3]	No change	**Disabled master**	**Disabled master**
Software application problem (lock-up or continual crashes)	Reboot as stack member	Re-elect master	Re-elect master
Software crash or lock-up	Frozen[4]	Re-elect master	Re-elect master
Power-down or PSU failure	Powered down	Re-elect master	Re-elect master

Table 81-1: State change table

Event on Stack Member Node	Reaction on Master	Reaction on Stack Member	Reaction on Stack Member
Both stack links removed	No change	**Disabled master**[1]	Re-elect master [2]
Hardware reset (or fault)	No change	Reset/offline	Reset/offline
Run the **no stack enable** command[3]	No change	**Disabled master**	**Disabled master**
Software application failover (lock-up or continual crashes)	No change	Re-boot as backup member	Reboot as stack member
software crash or lock-up	No change	Frozen[4]	Frozen[4]
Power-down / PSU failure	No change	Powered Down	Powered down

If a backup member becomes the **Disabled master** it will first disable all its switch ports, then activate any triggers specified with the **type stack disabled-master** command that have been configured.

1. The stack member assumes the role of stack master. In specific situations this condition could result in a stack containing two masters. This would present problems with network management and the control of links that were previously aggregated.
2. The following situation will apply to a switch that has been removed from the stack by the using the “no stack enable” command:
   - « The switch will be unaware of further faults within the stack it was previously a member of.
   - « Should this switch then be powered down, all links previously shut down (as a result of running the no stack enable command) will remain down.
3. If the backup member’s ports are still up, this may cause downstream switches with trunked ports to operate incorrectly.

Stack Failure Recovery

If the stack master either fails, or is removed, the other stack members will re-elect a new stack master. The stack members automatically determine which of them becomes the new stack master. See the **Disabled Master Monitoring (DMM)** and the **Disabled master** sections for more information. Alternatively, you can manually configure a trigger with the **type stack disabled-master** command on page 76.28 to activate on a stack member if it becomes the disabled master.

Table 81-1 shows how the stack backup members would respond to various problems occurring on the stack master stack.

Note

When VCStack is used with EPSR, the EPSR **failovertime** must be set to at least 5 seconds to avoid any broadcast storms during failover. Broadcast storms may occur if the switch cannot failover quickly enough before the EPSR **failovertime** expires. See the **epsr** command for further information about the EPSR **failovertime**.

See the **reboot rolling** command for further information about stack failover.

Stack Separation and Recovery

Stack stubs occur when a fault results in the stack splitting into two, with one of the stack members taking on the role of stack master. Where the stack master is still active after a fault, and other stack members are not aware that the stack master is still active, the result can be two independently operating stacks, or stubs.

When two stub stacks are reconnected, a dual master situation will be detected, and the console log will display the message that a 'duplicate master' was detected. This situation results in the re-election of the stack master based upon the lowest Priority ID, or, where both members have the same Priority ID, the lowest MAC address. The 'losing' master and other prospective stack members will then reboot and join the new stack as backup stack members.

Note Stubs are unlikely to cause network connectivity problems if a resiliency link is used.

Stack Maintenance

Adding a stack member

An unstacked switch can be added to an existing stack (hot-swapped in) with minimal impact on traffic. To do this, power down the new member switch, then connect its stacking ports and power on the switch. The switch will boot as a member of the stack.

Note The existing Stack Member-ID and the device MAC address will have no effect on the status of the new member switch. The stack will admit the new device as an ordinary stack member and allocate it a new Stack Member-ID if its ID is one that already exists.

However, for good practice we recommend pre-configuring the new member with settings that are appropriate for when the new switch becomes a stack member.

This is to avoid unexpected situations occurring when the stack is rebooted.

For example, if the new member had a priority setting that was lower than 128 and all the existing stack members were configured with the default; then, when the stack is rebooted, the new member would be elected as the stack master.

Replacing a stack member

A stack member can be removed from a stack (hot-swapped out) with minimal impact on stack traffic. To do this, power-down the stack member, and disconnect its stacking ports.

You can seamlessly swap a stack member switch into the stack to replace another with the same configuration. This provides a simple way to replace an out-of-service switch with minimal impact, and minimal administration requirement. Before inserting the replacement device into the stack, make sure that:

- The replacement device is running a compatible firmware version.
- You set the Stack ID on the replacement device to the same ID as the device being replaced.

Once these requirements are met, insert the new stack member, reconnect the stacking ports and power-up the new stack member.

Combining separate stacks

Two small (2 member) stacks can be combined into a single 4 member stack by physically reconnecting the stack members and rebooting. Note that the likelihood of a successful stack recombination is greatly increased if you set the stack IDs of each stack member to be unique within the combined stack that you are creating.

For example, consider two individual 2 member stacks that are to be combined into one 4 member stack, where the members of each stack had the stack member IDs of 1 and 2. Then, before you combine the stacks, you should renumber the member IDs of stack two to be 3 and 4.

Disabled master

A properly functioning VCStack contains an (active) master and one or more (backup) members. Under fault conditions it is possible for some of the stack members to lose connectivity with the stack master. In this situation the stack members without master connectivity will form themselves into a stack stub and elect a “Disabled Master” to manage the stub until the fault is rectified. Once elected to this state the disabled master will disable all of its own ports and those of all other stack members within the stub. Apart from this, the operation and ‘look and feel’ of a disabled master is very similar to an active master.

By disabling all the stub’s switchports, the disabled master avoids potential network connectivity problems that could result from by having two stack masters using the same configuration, or two switches in separated stubs trying to share the same “logical” communications paths such as a non functioning aggregated links. The active master’s ports are unaffected by this, and they will continue to forward traffic normally.

Note that status information for members of the stack stub can be accessed by logging into the disabled master, in the same way as obtaining status information for a normal stack.

Note

In a stack of more than two units, several stack members could become separated from the stack master. In this case, these stack members will form a stack stub together. Only one stack member will become the disabled master. The other switches will remain as backup stack members, but their switchports will still be disabled. Status information for the stack members can be accessed by logging into the disabled master, in the same way as obtaining status information for a normal stack.

Disabled Master Monitoring (DMM)

The stack resiliency link and disabled master state offer a unique prevention of catastrophic network connectivity problems. However, when stack members become separated, the network is still left in a fragile state where the stack master no longer has the redundancy of a backup stack member. If the original stack master were to subsequently fail whilst the stack was separated, then all network connectivity would be lost if the disabled master's switchports remained shut down.

The Disabled Master Monitoring (DMM) feature avoids this situation by continuing to monitor the status of the original stack master (the active master) via the stack resiliency link. When the DMM feature is enabled, the disabled master can detect a failure of the original stack master within a few seconds. If a failure is detected, the disabled master transitions to the active master state and automatically re-enables all its switchports. This allows traffic forwarding via the stack to continue.

For more information about the disabled master state, see the section **"Disabled master" on page 81.17**. Note that a disabled master has the same configuration as an active master, but a disabled master has all its links shut down.

Table 81-2: Stack behavior comparison

Stack behavior with DMM disabled	Stack behavior with DMM enabled
■ The VCStack breaks with the Stack Resiliency Link configured and enabled.	■ The VCStack breaks with the Stack Resiliency Link configured and enabled.
■ The separated stack member becomes a disabled master.	■ The separated stack member becomes a disabled master.
■ The disabled master does not monitor the active master.	■ The disabled master monitors the active master.
■ If the active master fails then the disabled master does not become the active master (no state transition).	■ If the active master fails then the disabled master becomes the active master (disabled to active transition).
■ No switchports are re-enabled on the disabled master. No traffic is forwarded.	■ Switchports on the disabled master are re-enabled. Traffic is still forwarded.

To enable the DMM feature, use the commands:

```
awplus# configure terminal
awplus(config)# stack disabled-master-monitoring
```

To disable the DMM feature, use the commands:

```
awplus# configure terminal
awplus(config)# no stack disabled-master-monitoring
```

To show the status of DMM on the VCStack, use the command:

```
awplus# show stack [detail]
```

To apply a trigger upon transition from active master state to disabled master state, use the command:

```
awplus# type stack disabled-master
```

To apply a trigger upon transition from disabled master state to active master state, use the command:

```
awplus# type stack master-fail
```

Note

A disabled master trigger allows you to specify a script to reconfigure the disabled master on the fly, should a catastrophic failure separate the stack. This is useful to configure an alternate IP address so you can still log in to the disabled master via an SSH or a Telnet connection. The trigger script should use the **no shutdown** command to re-enable any switchports needed for an SSH or a Telnet management connection.

Provisioning (Stack Members)

Stack member provisioning is the pre-configuration of a stack member's position ready for insertion at a later time. Provisioning enables a network administrator to pre-configure vacant stack member capacity within a VCStack, ready to be hot-swapped in at a later time. Later, when the stack member switch is physically added, its configuration is automatically applied with the minimum network disruption. Provisioning is ON by default, and cannot be disabled.

Provisioned capacity can be applied by either of the following actions:

- applying the **switch provision (stack)** command on page 82.26
- installing, then removing a provisionable device from its physical location, that is, a switch from its stack.

Provisioned Board Classes

Provisioning introduces the concept of defined board classes. **Table 81-3** lists the stack member classes that have been defined for provisioning. Each board class is assigned a class and an appropriate port count. Presently no further definitions have been made for additional features such as media type, or PoE capability. This structure simplifies configuration.

Table 81-3: Provisioned stack member classes

Board Classes	
Class	Port Count
GS924MX	24 switch ports, plus 4 SFP+ ports, two of which can be used for VCStacking.
GS924MPX	24 switch ports, plus 4 SFP+ ports, two of which can be used for VCStacking. Also has Power over Ethernet.
GS948MX	48 switch ports, plus 4 SFP+ ports, two of which can be used for VCStacking.
GS948MPX	48 switch ports, plus 4 SFP+ ports, two of which can be used for VCStacking. Also has Power over Ethernet.

Applying Hardware Provisioning

As previously mentioned, provisioning is the pre-configuration of vacant (i.e. unused) device capacity ready for device insertion at a later time.

Without provisioning

On software versions prior to version 5.3.4, trying to configure an unused port will result in the following error message:

```
awplus(config)# interface port4.0.1
% Can't find interface port4.0.1
```

With provisioning

With provisioning, you can configure stack members and their ports ready for future addition, even though they are not currently physically present:

```
awplus(config)# switch 2 provision <switch-model>
```

For information on using this command, see **"switch provision (stack)" on page 82.26**.

Now that the switch is provisioned within the stack—although not yet physically present—you can move on to provisionally configure the switch ports themselves. The following example sets the port speed of port 2.0.1 to be 1000 Mbps.

```
awplus(config)# interface port2.0.1
awplus(config-if)# speed 1000
```

You can apply provisional configuration to all interface related commands. However, you cannot apply provisioning where it changes the network's physical topology. For example, you can't provision a switch as stack member 3 and then later change it - while its position is still vacant - to stack member 4. In this situation, you would need to unprovision the switch, then provision it again as stack member 4.

The following example creates a provisioned configuration that shows the association of ports with a VLAN:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 12 state enable
awplus(config-vlan)# exit
awplus(config)# interface port2.0.1
awplus(config-if)# switchport mode access
awplus(config-if)# switchport access vlan 12
awplus(config-if)# exit
awplus(config)# interface port2.0.2-port2.0.26
awplus(config-if)# switchport mode access
```

Provisioning error messages

The following error messages may appear when configuring provisioning:

Table 81-4: Provisioning error messages (switch x [bay y] provision)

Error Message	Comment
`Switch %d must be provisioned before bays can be provisioned.`	`%d` = stack member id
`% Switch %d (%s) has 0 expansion bays.`	`%d` = stack member id `%s` = board class
`% Board class %s is incompatible with this system.`	`%s` = board class from cmd line
`% switch %d is already populated with %s.`	Indicates an attempt to provision a switch that is already present.
`% switch %d is already provisioned for %s.`	Indicates an attempt to provision a switch that is already provisioned.

Table 81-5: Provisioning error messages (no switch x [bay y] provision)

Error Message	Comment
`% switch %d bay %d is currently populated by %s`	You must remove hardware before unprovisioning

Removing Hardware Provisioning

Hardware capacity that has been previously provisioned and is presently unoccupied can be unprovisioned with the no switch provision command. This removes the provisioned configurations for hardware that has either not yet been physically added to a switch or VCStack, or has previously existed, but has been removed.

The no switch provision command will also delete any switch bay commands with the same unit number and all associated interfaces, as well as all configuration for that switch.

You cannot unprovision hardware that is currently installed. A no switch command will not succeed if the unit/unit.bay location is currently occupied. For example:

```
awplus(config)# no switch 2 bay 2 provision

                % switch 2 bay 2 is currently populated by
                <module-type>
```

The following example displays the output of a show stack that includes a provisioned VCStack member 3:

```
Virtual Chassis Stacking summary information
ID  Pending ID  MAC address      Priority  Status   Role
1   -           0000.cd28.5377   128       Ready    ActiveMaster
2   -           0000.cd29.95bf   128       Ready    BackupMember
3   -           0000.0000.0000   -         -        Provisioned
```

Switch ID 3 is then unprovisioned:

```
awplus(config)# no switch 3 provision
```

Run the show stack command to confirm that switch 3 has been unprovisioned:

```
awplus# show stack
```

```
Virtual Chassis Stacking summary information
ID  Pending ID  MAC address      Priority  Status  Role
1   -           0000.cd28.5377   128       Ready   ActiveMaster
2   -           0000.cd29.95bf   128       Ready   BackupMember
```

Note Ensure that you save your running configuration to your startup configuration after making any provisioning changes using **copy running-config startup-config.**

Displaying Provisioned Configurations

In this respect the major difference associated with provisioning, is that interface configurations will still exist in the config files and will appear in show commands, even though a device itself may not be physically installed. This (provisioning) could result from device capability that has been preconfigured for future installation, or could result from the removal of an installed device.

The show running-config command includes switch commands for existing hardware, plus all non-existent, but provisioned, hardware. The following example output of the show running-config command illustrates how provisioned and existing hardware is displayed.

Figure 81-10: Sample display of existing and provisioned show output

```
sh running-config
!
switch 1 provision GS948MX
!
interface port1.0.1-1.0.12
 switchport
 switchport mode access
!
.end
```

Displaying provisioned hardware status

The status, present or provisioned, appears in monitoring commands such as the show interface brief command. The following sample output from the show interface brief command shows the provisioning status of two configured stack members.

Figure 81-11: Sample show interface brief output showing hardware provisioning status

```
awplus#show interface brief
Interface              Status          Protocol
port2.0.24             admin up        down
port3.0.1              admin up        provisioned
port3.0.2              admin up        provisioned
```

A more detailed inspection of the provisioned port2.0.3 is shown below. Note that the MAC address is 0000.0000.0000, which is the value applied as a placeholder for all provisioned ports. Also note that although the port is in the link DOWN state its administrative state of UP PROVISIONED means that it can be further configured. For example, it can be associated with a VLAN, or added to a link aggregation group.

Figure 81-12: Sample display showing provisioning status of a specific port

```
Interface port2.0.3
  Scope: both
  Link is DOWN, administrative state is UP PROVISIONED
  Thrash-limiting
    Status Unknown, Action learn-disable, Timeout 1(s)
  Hardware is Ethernet, address is 0000.0000.0000
  index 6801 metric 1 mtu 1500 mru 1522
  <BROADCAST,MULTICAST>
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast
pks0
```

Provisioning and Configuration Management

A benefit of provisioning is configuration settings are no longer dependent on the existence of hardware devices. When a device is removed, all the interfaces for that device are shut down and its provisioning status is set. This means that you can add or remove physical hardware without affecting your network interfaces. Of course when ports go down (i.e. are physically removed) there will be other changes to network configuration, as protocols may re-converge or routes may be removed.

Switches within a VCStack can be hot-swapped without the need for reconfiguration.

The configuration of a newly inserted device that matches the provisioned board-class is achieved on a best-effort basis. For example inserting a non-POE switch into a stack member location configured for PoE will result in the failure of the PoE configuration commands.

Take care that your provisioned configurations, match with the type of hardware that you plan to install.

```
awplus(config)# switch 2 bay 4 provision <product-type>
awplus(config)# interface port2.0.4
awplus(config-if)# shutdown
```

Software Version Auto Synchronization

Introduction

Different software releases exhibit functional and operational differences. To maintain consistent behavior across the stack, all new member switches must be running the same software release before they can fully join the stack.

Manually upgrading the software release of each new stack member that joins a stack would be a cumbersome process. The VCStack software version auto synchronization feature automates this process by ensuring the same software release is used on all stack members, and automatically upgrades stack members where required.

How Auto Synchronization Works

Software version comparison

When the stack is formed, it elects one of its switches to become the master. The software release running on the stack master will then become the software version used throughout the stack. After a master is elected, all the stack members compare their current software version with the version that is running on the stack master.

If the comparison process detects differences between software versions, the software version auto synchronization feature will automatically copy the master's software release onto the appropriate stack members. Once the software release has successfully been copied, this version will become the boot software for that particular stack member, which will then reboot in order to load the new software release.

When auto-synchronization upgrades a stack member, the member's current running software will be set as the backup software release. If there are any problems loading the new software, then the backup software release will be used to recover.

If the stack member does not have enough free Flash memory space for the new release, then the new release will replace up to two older release files in Flash memory, which is determined by software build dates of the older release files. The oldest release files are replaced first.

Auto synchronization limitations

Because the stack master's software version gets applied to the rest of the stack, care must be taken to ensure the correct switch is elected master. If the master is running an older software release, then software version auto synchronization may downgrade the software releases running on other stack members. For configuring which stack member becomes the master, see the **stack priority command on page 82.19**.

Software version auto synchronization will not work if stack members are booting using either a one-off boot or from TFTP or YMODEM. In these situations, any stack members running different software will boot as standalone devices.

Incompatible software releases

The software version auto synchronization feature will not always work if there have been significant VCStack or system changes between the two different software releases. The VCStack discovery of other stack members uses an internal “stack S/W version” to detect compatibility between builds.

If the VCStack software between two stack members is incompatible, the software version auto synchronization feature will not work. Instead, an “incompatible stack S/W version” log message will be displayed and both stack members will boot as standalone devices. This is an undesirable situation because both devices may load the same configuration file, which could cause network conflicts. In order to avoid this situation when upgrading the stack to a new major release, ensure the “boot system” command succeeds.

In general, the software version auto synchronization feature will work between maintenance releases, such as between 5.4.4-0.1 and 5.4.4-0.2, but may not work between major or minor releases that have new VCStack features, such as between 5.4.3-0.1 and 5.4.4-0.1. For information about which specific releases support auto synchronization, see the **New and Enhanced Features** document for the release.

Upgrading stack software reliably

When upgrading a stack to a new software release, the **boot system backup** command on page 7.11 will automatically synchronize the new software release across stack members. If there is insufficient file space on a backup member, the boot system command has an interactive mode that prompts you to delete old releases to free up file space.

However, if you choose not to delete any release files, or if Flash space is taken up with other types of files, then the boot system command can fail to set the preferred release on the backup member. If you do not have enough space in Flash to add a backup release file, then remove unused files in Flash using the delete command.

If you are unsure which files to delete, the following process may assist you.

```
awplus# remote-login 2
awplus-2# enable
awplus-2# dir
```

Use the remote-login command to login to the backup member with insufficient free file space, in this example member 2.

Look for any .rel (release) files, .jar (GUI), or .tgz and .gz (diagnostic) files that are no longer needed and use the delete command to remove them.

Alternatively, you can use the file system commands directly from the master's console prompt using the filepath of the backup member's Flash. Substitute `awplus` for the hostname in the configuration, and use `awplus-2` for stack member 2, and so on.

```
awplus# dir awplus-2/flash:*
awplus# delete awplus-2/flash:/GS900-5.4.4E-
        1.1.rel
```

Chapter 82: Stacking Commands

Introduction 82.2
Command List 82.3
clear counter stack 82.3
reboot rolling 82.4
reload rolling 82.4
remote-login 82.5
show counter stack 82.6
show provisioning (stack) 82.10
show stack 82.11
stack disabled-master-monitoring 82.15
stack enable 82.16
stack management subnet 82.17
stack management vlan 82.18
stack priority 82.19
stack renumber 82.20
stack renumber cascade 82.21
stack resiliencylink 82.22
stack virtual-chassis-id 82.24
stack virtual-mac 82.25
switch provision (stack) 82.26
switchport resiliencylink 82.27

Introduction

This chapter provides an alphabetical reference for each of the Stacking commands.

Also note the following stacking trigger commands that are documented in the Triggers chapter:

type stack disabled-master command on page 76.28

type stack master-fail command on page 76.30

type stack member command on page 76.31

type stack link command on page 76.29

In addition to the stacking commands shown in this chapter, stacking content also exists in the following commands:

hostname command on page 8.17

reboot command on page 8.22

reload command on page 8.23

show cpu command on page 8.25

show cpu history command on page 8.28

show exception log command on page 10.36

show file systems command on page 7.36

show memory command on page 8.35

show memory history command on page 8.38

show process command on page 8.42

show system command on page 8.46

Caution

Stack operation is only supported if stack virtual-mac is enabled. For more information refer to: "Enabling the stack virtual-mac" on page 81.13 and "stack virtual-mac" on page 82.25

Command List

clear counter stack

This command clears all stack counters for all stack members.

Syntax `clear counter stack`

Mode Privileged Exec

Example To clear all stack counters:

```
awplus# clear counter stack
```

Related Commands show counter stack

reboot rolling

This command reboots a stack in a rolling sequence to minimize downtime.

The stack master is rebooted, causing the remaining stack members to failover and elect a new master. The rebooted unit remains separate from the remaining stack and boots up as a stand-alone unit. Once the rebooted unit has finished running its configuration and has brought its ports up, it reboots all the remaining stack members at once.

Syntax `reboot rolling`

Mode Privileged Exec

Usage If you are upgrading to a new software version, the new version must also support rollling reboot.

When stacking is used with EPSR, the EPSR **failovertime** must be set to at least 5 seconds to avoid any broadcast storms during failover. Broadcast storms may occur if the switch cannot failover quickly enough before the EPSR **failovertime** expires. For further information about EPSR **failovertime**, see the **epsr** command on page 58.4.

Examples To rolling reboot the stack, use the following commands:

```
awplus# reboot rolling
Continue the rolling reboot of the stack? (y/n):
```

After running this command, the stack master will reboot immediately with the configuration file settings. The remaining stack members will then reboot once the master has finished re-configuring.

```
Continue the rolling reboot of the stack? (y/n):
awplus# y
```

Related Commands **boot system**
epsr

reload rolling

This command performs the same function as the **reboot rolling** command on page 82.4.

remote-login

This command is used only on the master in order to log onto the CLI of another stack member. In most respects the result of this is similar to being logged into the stack master. Configuration commands are still applied to all stack members, but show commands, and commands that access the file system are executed locally.

The specific output obtained will vary greatly depending on the show command chosen.

Syntax `remote-login <stack-ID>`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Mode Privileged Exec

Usage Note that some commands such as **ping** or **telnet** are not available when the remote-login is used.

Example To log onto stack member 2, use the following command:

```
awplus# remote-login 2
```

To return to the command prompt on the master stack member, type **exit**.

show counter stack

Use this command to display stack related counter information.

Syntax `show counter stack`

Default All counters are reset when the stack member is rebooted.

Mode User Exec and Privileged Exec

Usage This displays the stacking counter information for every stack member.

Examples To display the stacking counter information about the whole stack, use the following command.

```
awplus# show counter stack
```

Figure 82-1: Example output from the show counter stack command

```
Virtual Chassis Stacking counters

Stack member 1:

Topology Event counters
Units joined          ......... 1
Units left            ......... 0
Links up              ......... 1
Links down            ......... 0
ID conflict           ......... 0
Master conflict       ......... 0
Master failover       ......... 0
Master elected        ......... 1
Master discovered     ......... 0
SW autoupgrades       ......... 0

Stack Port 1 Topology Event counters
Link up               ......... 3
Link down             ......... 2
Nbr re-init           ......... 0
Nbr incompatible      ......... 0
Nbr 2way comms        ......... 1
Nbr full comms        ......... 1

Stack Port 2 Topology Event counters
Link up               ......... 0
Link down             ......... 0
Nbr re-init           ......... 0
Nbr incompatible      ......... 0
Nbr 2way comms        ......... 0
Nbr full comms        ......... 0
```

Figure 82-1: Example output from the show counter stack command (cont.)

```
Topology Message counters
Tx Total                ......... 4
Tx Hellos               ......... 4
Tx Topo DB              ......... 0
Tx Topo update          ......... 0
Tx Link event           ......... 0
Tx Reinitialise         ......... 0
Tx Port 1               ......... 4
Tx Port 2               ......... 0
Tx 1-hop transport      ......... 4
Tx Layer-2 transport    ......... 0
Rx Total                ......... 1
Rx Hellos               ......... 1
Rx Topo DB              ......... 0
Rx Topo update          ......... 0
Rx Link event           ......... 0
Rx Reinitialise         ......... 0
Rx Port 1               ......... 1
Rx Port 2               ......... 0
Rx 1-hop transport      ......... 1
Rx Layer-2 transport    ......... 0

Topology Error counters
Version unsupported     ......... 0
Product unsupported     ......... 0
XEM unsupported         ......... 0
Too many units          ......... 0
Invalid messages        ......... 0

Resiliency Link counters
Health status good      ......... 1
Health status bad       ......... 0
Tx                      ......... 0
Tx Error                ......... 0
Rx                      ...... 3600
Rx Error                ......... 0

Stack member 2:

-- Output repeated for other stack members - details not shown--
```

Table 82-1: Parameters in the output of the show counter stack command

Parameters	Description
`Topology Event Counters`	
`Units joined`	Number of times that the stack acquires a member.
`Units left`	Number of times that the stack loses a member.
`Links up`	Number of times that a stack link is up in the stack.
`Links down`	Number of times that a stack link is down in the stack.
`ID conflict`	Number of times that stack-ID conflicts.
`Master conflict`	Number of times that stack master conflict occurs.
`Master failover`	Number of times that stack master fails.
`Master elected`	Number of times that stack master is elected.
`Master discovered`	Number of times that stack master is discovered.
`SW autoupgrades`	Number of times that the software in the stack members are auto upgraded.
`Stack port counters`	

Table 82-1: Parameters in the output of the show counter stack command (cont.)

Parameters	Description
`Link up`	Number of times that this unit's physical stack link has come up.
`Link down`	Number of times that this unit's physical stack link has come down.
`Nbr re-init`	Number of times that the neighbor is detected as having reinitialised.
`Nbr incompatible`	Number of times that the neighbor is detected as incompatible.
`Nbr 2way comms`	Number of times that the neighbor is in two way communication status.
`Nbr full comms`	Number of times that the neighbor is in full communication status.
`Topology message counters`	
`Total`	Total number of topology messages.
`Hellos`	Number of hello messages.
`Topology DB`	Number of topology database messages.
`Topology update`	Number of topology database update messages.
`Link event`	Number of link event messages.
`Reinitialise`	Number of reinitialise messages.
`1-hop transport`	Number of 1-hop transport messages.
`Layer-2 transport`	Number of layer 2 transport messages.
`Link event`	Number of link event messages.
`Reinitialise`	Number of reinitialise messages.
`1-hop transport`	Number of 1-hop transport messages.
`Layer-2 transport`	Number of Layer 2 transport messages.
`Topology error counters`	Reasons why a neighboring unit could not join the stack.
`Version unsupported`	Number of stack software version unsupported errors.
`Product unsupported`	Number of product unsupported errors.
`XEM unsupported`	Number of XEM unsupported errors.
`Too many units`	Number of too many units errors.

Table 82-1: Parameters in the output of the show counter stack command (cont.)

Parameters	Description
`Invalid messages`	Number of invalid messages.
`Health status good`	The number of times that the resiliency link has successfully carried healthchecks following a failure at startup.
`Health status bad`	The number of times that the resiliency link healthcheck has timed out. A timeout occurs when a backup stack member detects a delay greater than two seconds between healthcheck messages received.
`Rx`	The total number of healthcheck messages that a stack member has received from the stack master.
`Rx Error`	The total number of invalid healthcheck messages that have been received from the master. This message is not applicable to the stack master.

Related Commands

show stack
switch provision (stack)

show provisioning (stack)

Use this command to display the provisioning status of all installed or provisioned hardware. Provisioning is the preconfiguration necessary to accommodate future connection of hardware items such as a switch.

Syntax `show provisioning`

Mode User Exec and Privileged Exec

Example To show provisioning, use the following command:

```
awplus# show provisioning
```

Output **Figure 82-2: Example output from the show provisioning command**

```
Switch provisioning summary information

ID   Board class Status
1.0  AT-GS924    Hardware present
```

Table 82-2: Parameters in the output of the show provisioning command

Parameter	Description
`ID`	The unit bay-location of the hardware provision.
`Board class`	The hardware type.
`Status`	The provisioned state: ■ Hardware Present means that the hardware is currently installed in the stack. ■ Provisioned means that although the hardware is not currently installed, the stack is preconfigured ready to accept the hardware installation.

show stack

Use this command to display information about current stack members.

Syntax `show stack [detail]`

Parameter	Description
`detail`	Display detailed stacking information.

Default Display summary information only.

Mode User Exec and Privileged Exec

Usage This command displays information about current stack members. If the **detail** parameter is specified, additional information will be displayed for each stack member. By default, only summary information is displayed.

Example To display summary information about the stack, use the command:

```
awplus# show stack
```

Output **Figure 82-3: Example output from the show stack command**

```
Virtual Chassis Stacking summary information

ID  Pending ID  MAC address      Priority  Status  Role
1   -           0000.cd28.07e1   128       Ready   Active Master
2   -           0015.77c2.4d44   128       Ready   Backup Member
3   -           0015.77c9.7464   128       Syncing Backup Member
4   -           -                -         -       Provisioned

Operational Status                Normal operation
Stack MAC address                 0000.cd28.07e1
```

Table 82-3: Parameters in the output from the show stack command

Parameter	Description
`ID`	Stack-ID.
`MAC address`	Stack member MAC address.
`Priority`	Stack member master election priority (between 0 and 255). Note that the lowest number has the highest priority.
`Role`	Stack member's role in the stack, this can be one of: ■ **Active Master** ■ **Disabled Master** — this is the temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a "type stack disabled-master" trigger. ■ **Backup Member** — a device other than the stack master. ■ **Provisioned** — indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.

Example To display the detailed stacking information about the stack's overall status:

```
awplus# show stack detail
```

Figure 82-4: Example output from the show stack detail command

```
Virtual Chassis Stacking detailed information

Stack Status:
----------------------------------------------------------------
Operational Status                      Normal operation
Management VLAN ID                      4094
Management VLAN subnet address          192.168.255.0
Virtual Chassis ID                      388 (0x184)
Virtual MAC address                     0000.cd37.0184
Mixed mode                              Disabled
Disabled Master Monitoring              Enabled

Stack member 1:
----------------------------------------------------------------
ID                                      1
Pending ID                              -
MAC address                             0000.cd28.070d
Last role change                        Wed May  7 22:31:58 2014
Product type                            AT-GS924MPX
Role                                    Active Master
Priority                                1
Host name                               awplus
S/W version auto synchronizaion         On
Resiliency link status                  Configured
Stack port 1.0.27 status                learned neighbor 2
Stack port 1.0.28 status                learned neighbor 3

Stack member 2:
----------------------------------------------------------------
ID                                      2
Pending ID                              -
MAC address                             0000.cd29.716d
Last role change                        Wed May  7 23:47:21 2014
Product type                            AT-GS924MPX
Role                                    Backup Member
Status                                  Ready
Priority                                2
Host name                               awplus-2
S/W version auto synchronization        On
Resiliency link status                  Successful
Stack port 2.0.27 status                learned neighbor 3
Stack port 2.0.28 status                learned neighbor 1

Stack member 3:
----------------------------------------------------------------
ID                                      3
Pending ID                              -
MAC address                             0015.77c2.4d9d
Last role change                        Wed May  7 22:31:58 2014
Product type                            AT-GS924MPX
Role                                    Backup Member
Priority                                3
Host name                               awplus-3
S/W version auto synchronizaion         On
Resiliency link status                  Successful
Stack port 3.0.27 status                learned neighbor 1
Stack port 3.0.28 status                learned neighbor 2
```

Table 82-4: Parameters in the output from the show stack detail command

Parameter	Description
`Host name`	The host name of the stack member.
`ID`	Stack-ID.
`Last Role Change`	The date and time the stack member last changed its role in the stack.
`MAC address`	Stack member MAC address.
`Management VLAN ID`	The VLAN ID currently used for stack management: the default is 4094.
`Management VLAN subnet address`	The current stacking management VLAN subnet address.
`Virtual Chassis ID`	The Virtual Chassis ID determines the last 12 bits of the Virtual MAC address: `0000.cd37.0xxx`
`Virtual MAC Address`	The Virtual MAC address of the stack.
`Disabled Master Monitoring`	The current Disabled Master Monitoring status. This can be: ■ **Enabled** ■ **Disabled** ■ **Inactive**
`Operational Status`	The status of the stack. This can be: ■ **Normal operation**: If any other status is displayed, it may warrant further investigation. ■ **Stacking hardware disabled:** The **stack enable** command needs to be added to the configuration to activate the stacking feature. ■ **Operating in failover mode**: This stack member has become separated from the rest of the stack, or it failed to join the stack correctly. ■ **Standalone unit**: Stacking is enabled, but no other stack members are present. ■ **Not all stack ports are up**: One or more stacking ports may be down, or stacking discovery may not have detected the neighbor successfully.
`Stack Status`	The stack's overall status. Note that a warning is issued if the stack is not connected in a standard ring topology.
`Pending ID`	The pending stack member ID. This can be changed by the **stack renumber** command on page 82.20. If there is no pending ID, the "–" symbol will display.

Table 82-4: Parameters in the output from the show stack detail command (cont.)

Parameter	Description
`Stack port status`	The status of the stack port. This can be: ■ **Down** ■ **Neighbor incompatible** ■ **Discovering neighbor** ■ **Learned neighbor**
`Priority`	Stack member master election priority (between 1 and 255) Note that the lowest number has the highest priority.
`Product Type`	Stack member product type.
`Provisioned`	Indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.
`Resiliency link status`	The current status of the resiliency link. The status can be one of: ■ **Not configured** (Master or Member). ■ **Configured** (Master only). ■ **Successful**: Successfully receiving healthchecks from the Active Master. ■ **Failed** (Member only): Not receiving any healthchecks from the Active Master. ■ **Stopped**: The resiliency link is configured, but is inactive. This may occur in a Disabled Master stack, for example if the Disabled Master Monitoring feature is not used.
`Role`	Stack member's role in the stack, this can be one of: ■ **Active Master**. ■ **Disabled Master** — The temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a "**type stack disabled-master**" trigger command. ■ **Backup Member** — a device other than the stack master. ■ **Discovering** — joining the stack.
`Status`	Indicates how readily a stack member can take over as master if the current stack master were to fail. ■ **Init** — the stack member is completing the startup initialization. ■ **Syncing** — the stack member is synchronizing state information with the stack master following startup. ■ **Ready** — the stack member is fully synchronized with the current master and is ready to take over immediately.

Related Commands

show counter stack
stack disabled-master-monitoring
stack resiliencylink

stack disabled-master-monitoring

This command enables the Disabled Master Monitoring (DMM) feature. If a stack member becomes a disabled master, the DMM feature will use the stack resiliency link to continue monitoring the health of the separated stack master.

Use the **no** variant of this command to disable the DMM feature.

Syntax

```
stack disabled-master-monitoring
no stack disabled-master-monitoring
```

Default By default, Disabled Master Monitoring is enabled. However, it only operates if there is a resiliency link.

Mode Global Configuration

Usage This command enables additional stack resiliency link functionality, which is used if a stack separation occurs. For DMM to operate, a resiliency link must also be configured (**stack resiliencylink** command on page 82.22). A stack separation could result in a stack member becoming a disabled master, which has the configuration as a normal stack master except that all its switchports are shutdown.

For more information about the disabled master state, see **"Disabled master" on page 81.17**.

When the DMM feature is enabled, the disabled master will continue to monitor the health of the original stack master over the stack resiliency link connection. If the original stack master were to fail, when the DMM feature is enabled, then the disabled master will detect this and will automatically re-enable its switchports. This ensures that the stack will continue to pass network traffic, even if a catastrophic stack failure occurs.

For more information about the DMM feature when the stack member is a disabled master, see **"Disabled Master Monitoring (DMM)" on page 81.18**.

Examples To enable the DMM feature, use the following commands:

```
awplus# configure terminal
awplus(config)# stack disabled-master-monitoring
```

To disable the DMM feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no stack disabled-master-monitoring
```

Related Commands

switch provision (stack)
show stack
stack resiliencylink
type stack disabled-master
type stack master-fail

stack enable

This command is used on a stackable stand-alone switch to manually turn on the VCStack feature.

This command can also be run on a switch that has previously been removed from a stack (by using the **no** variant of this command) and return it to stacking operation.

The **no** variant of this command removes a selected stack member switch, as specified by the *<stack-ID>* selection in the command syntax, from the virtual chassis stack.

Syntax

```
stack enable
no stack <stack-ID> enable
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.

Default The VCStack feature is enabled by default. The feature automatically starts when hardware is present.

Mode Global Configuration

Usage When stack enable is entered, the **stack virtual-mac** is automatically enabled. Using virtual-mac is required in order to minimize disruption on failover.

Running the **no** variant of this command will remove the selected stack member from the stack. At this point the removed member will act as a stand-alone master and will disable all of its ports. The switch can then only be accessed via its console port. If the command is run on the master then all current members of the stack will be disabled.

To return the switch to stack membership, first connect to the switch via its console port, then run the **stack enable** command. Then save the configuration and run the **reboot** command on page 8.22. This will reboot the switch and it will re-join the stack as an ordinary member.

If the switch was previously the stack master, you might want to return it to its original stack master status. To do this you must run the **reboot** command on page 8.22 again. This time—because the switch is now a stack member—the command will reboot the whole stack and result in a new master election.

Note the following condition of applying the **no stack** *<stack-ID>* **enable** command:

- If the specified `stack-ID` is not used by any current stack member, the command will be rejected.

Caution Disabling a stack member can significantly degrade the throughput capability of the stack.

Example To turn on stacking on a stackable stand-alone unit, use the command:

```
awplus# configure terminal
awplus(config)# stack enable
```

Related Commands **reboot**

stack management subnet

This command configures the subnet address used by the stack management VLAN.

Use the **no** variant of this command to reset the stack's VLAN subnet management address back to the default address and mask (192.168.255.0/27).

Syntax

```
stack management subnet <ip-address>
no stack management subnet
```

Parameter	Description
<ip-address>	The new subnet address for the stack management VLAN.

Default The default stacking management VLAN subnet address is 192.168.255.0 with a subnet mask 255.255.255.224 or /27.

Mode Global Configuration

Usage This command configures the stack management VLAN subnet address.

The management VLAN will be used for high speed communication between stacked units via the stacking ports. Although this command enables you to change the IP address command, the subnet mask must always remain as shown.

The stack management IP subnet is solely used internally to the stacked devices, and cannot be reached external to the stack. You should only change the stack management VLAN subnet address if it causes a conflict within your network.

Note that several separate stacks can use the same default management VLAN subnet address even though their user ports may share the same external network. If the stack subnet address is changed, then the configuration for any new units must also be updated before they are inserted into the stack.

If the management VLAN subnet address is changed by this command, you can use the **no** variant of this command to reset it to it's default.

Example To set the management VLAN subnet address to 192.168.255.144:

```
awplus# configure terminal
awplus(config)# stack management subnet 192.168.255.144
```

Related Commands stack management vlan

stack management vlan

Use this command to configure the stack management VLAN ID.

Use the **no** variant of this command to change the stack management VLAN ID back to the default (VLAN ID 4094).

Syntax

```
stack management vlan <2-4094>
no stack management vlan
```

Parameter	Description
<2-4094>	Stack management VLAN ID.

Default VLAN ID 4094

Mode Global Configuration

Usage The management VLAN is used for high speed communication between stacked units. This command enables you to change the ID of this VLAN.

The default stacking management VLAN ID is 4094, which is the last configurable VLAN ID in the switch.

The stack management VLAN is created and configured automatically so that the stack VLAN cannot be used in the stack's VLAN configuration commands (such as `awplus(config-vlan)# vlan <Stack management VLAN ID>`).

The management VLAN should only be changed if the default stack VLAN ID needs to be used in the stack's VLAN configuration.

Caution

When the command is entered, the updated management VLAN configuration will take effect once the stack is restarted.

If the management VLAN ID is changed by this command, you can use the no variant of this command to change it back to default value.

Examples To set the management VLAN to 4000, enter the following commands:

```
awplus# configure terminal
awplus(config)# stack management vlan 4000
```

To reset the management VLAN back to the default (4094), enter the following commands:

```
awplus# configure terminal
awplus(config)# no stack management vlan
```

Related Commands stack management subnet

stack priority

Use this command to change a specific stack member's master-election priority.

Syntax

```
stack <stack-ID> priority <0-255>
no stack <stack-ID> priority
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.
priority	The stack member's election priority value.
<0-255>	The stack member's new priority value. The lowest value is assigned the highest priority. The default is 128.

Mode Global Configuration

Usage This command is used to change the value of a specific stack member's master-election priority. If the specified stack-ID is not used by any current stack member, the command will be rejected.

The election criteria selects the stack member with the lowest priority value to become the stack master. Where two stack members both have the same lowest priority value, then the stack member with the lowest MAC address will be elected as master.

Note

Assigning a new priority value will not immediately change the current stack master. In order to force a master re-election after the new priority value is assigned, use reboot stack-member <master's ID> to reboot the current stack master, a new stack master will then be elected based on the new priority values.

Example To change the priority of stack member 2 to be 3, use the command:

```
awplus# configure terminal
awplus(config)# stack 2 priority 3
```

Validation Command show stack

stack renumber

Use this command to renumber a specific stack member.

Syntax `stack <existing stack-ID> renumber <new stack-ID>`

Parameter	Description
<existing stack-ID>	We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.
`renumber`	Change the existing `stack-ID`.
<new stack-ID>	We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.

Default Every stack unit will initially try to use a `stack-ID` of 1.

Mode Global Configuration

Usage This command is used to change the ID of a specific stack member - primarily when exchanging stack members. The changes made by this command will not take effect until the switch is rebooted.

Note

This command does not alter any of the stacks's existing configuration, apart from the `stack-ID` specified. For example, if stack member 2 were removed from the stack and a new stack unit is assigned the member 2 `stack-ID`, then the interface configuration that existed for the removed stack member 2 will be applied to the new stack member 2.

The ***existing stack-ID*** must already be assigned to an existing stack member. To avoid duplicating IDs, a warning message will appear if you assign a ***new stack-ID*** that is currently assigned to another stack member. However, you can continue to renumber the stack-IDs and remove ID duplications. If you do not remove the duplications, then one of the devices will be forced to automatically renumber to an unused ID. Once you have removed any duplicate IDs, you can reboot the switch to implement your changes.

Note that the configured `stack-ID` is saved immediately on the renumbered member, and so is not reliant on using the **copy running-config** command for it to take effect.

Example To renumber stack 1 to stack 2, use the commands:

```
awplus# configure terminal
awplus(config)# stack 1 renumber 2
```

Validation Command **show stack**

stack renumber cascade

This command is used to renumber the members of a stack so that their IDs are ordered sequentially, relative to the member's physical position within the stack.

Caution

Changing the stack numbering will upset the existing stack member configurations such as port settings. This command is intended for use when the stack is either initially commissioned, or has undergone a major reconfiguration. In this situation you run the stack renumber command (which will automatically reboot the switch), then configure the stack members to meet the new requirements.

Syntax

```
stack <stack-ID> renumber cascade [<stack-ID>]
```

Parameter	Description
<stack-ID>	The ID of the stack member to start renumbering from, from 1 to 4.
`renumber`	Change the existing stack-ID.
`cascade`	Renumber the existing stack-ID in cascade order.
<stack-ID>	The new ID for the first member renumbered, from 1 to 4.

Default If no stack-ID is specified, the member will take the default ID of 1.

Mode Global Configuration

Usage This command is used to renumber the members of a stack so that their stack-IDs are ordered sequentially. This would normally be done either when the stack is initially configured or following a major reconfiguration.

The renumber will start on the specified stack member. If that stack-ID is not used by any of the existing stack member, the command will be rejected.

The starting stack member will be renumbered with the new stack-ID specified, or the default of member ID of 1. The stack-ID of the next physically will be the starting members ID +1, for example member ID 2. This renumbering will continue in cascading order around the stack members.

The changes will take place immediately and reboot all stack members. For this reason a confirmation prompt follows this command entry, asking whether you are sure you want to renumber and reboot the entire stack.

Example

```
awplus(config)# stack 1 renumber cascade
Any existing interface configuration may no longer be valid
Are you sure you want to renumber and reboot the entire stack?(y/n):
y
```

Related Commands

show stack
switch provision (stack)
stack renumber

stack resiliencylink

This command configures the resiliency link used by the stack. The interface used may be either an eth port or is a dedicated VLAN (resiliencylink VLAN) to which switch ports may become members. This VLAN is dedicated to the resiliency link function and must not be the stack management VLAN.

Syntax `stack resiliencylink <interface>`

`no stack resiliencylink`

Parameters	Description
<interface>	The name of the interface that is connected to the resiliency link.

Mode Global Configuration

Usage The resiliency-link is only used when a backup member loses connectivity with the master via the stacking cables. Such a communication loss would occur if:

- a stacking link is removed or fails
- two or more stacking link cables are unplugged or fail
- the stack master itself fails due to a reboot or power failure

The resiliency-link allows the backup member to determine if the master is still present in the network by the reception of healthcheck messages sent by the master over the resiliency-link interface.

Reply healthcheck messages are received if the master is still online, but the stack will now split into two different “stubs”. The stub containing the existing master will continue operating as normal. The members in the masterless stub will now use a “type stack disabled-master” trigger to run a configuration to form a second temporary stack. This utilizes the remaining stack members' resources without conflicting directly with the master's configuration. If no “type stack disabled-master” trigger was configured on the switches, then the masterless stub members will disable their switch ports.

If no healthcheck messages are received, then the master is assumed to be completely offline, and so the other stack members can safely take over the master's configuration.

The purpose of the resiliency link is to enable the stack members (particularly the backup master) to check the status of the master under fault conditions. If the resiliency link is not configured, and the master loses communication with its other stack members, then the stack will assume the master is NOT present in the network, which could cause network conflicts if the master is still online. Note that this is a change to the stacking of releases prior to version 5.3.1.

Example To set the resiliency link to be VLAN 4093.

First use the **stack resiliencylink** command to create the resiliency `vlan 4093`

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next use the **switchport resiliencylink** command to assign the resiliencylink vlan to the interface port, in this case `port1.0.1`.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

Related Commands

show stack
switch provision (stack)
show stack detail
stack disabled-master-monitoring
switchport resiliencylink

stack virtual-chassis-id

This command specifies the stack virtual chassis ID. The ID selected will determine which virtual MAC address the stack will use. The MAC address assigned to a stack must be unique within its network.

Note The command will not take effect until the switch has been rebooted.

Syntax `stack virtual-chassis-id <id>`

Parameter	Description
<id>	The value of the ID - enter a number in the range 0 to 4095.

Mode Global Configuration

Usage The virtual-chassis-id entered will form the last 12 bits of a pre-selected MAC prefix component; that is, `0000.cd37.0xxx`. If you enable the stack virtual MAC address feature (by using the **stack virtual-mac** command) without using the **stack virtual-chassis-id** command to select the virtual-chassis-id, then the stack will select a virtual-chassis-id from a number within the assigned range.

Example To set the stack virtual-chassis-id to 63 use the commands

```
awplus# configure terminal
awplus(config)# stack virtual-chassis-id 63
```

This will result in a virtual MAC address of: `0000.cd37.003f`.

Related Commands
show running-config
show stack
switch provision (stack)
stack virtual-mac

stack virtual-mac

This command enables the stack virtual MAC address feature. For more information on this topic refer to **"Fixed or Virtual MAC Addressing" on page 81.13**. With this command set, the value applied for the virtual MAC address is determined by the setting of the command **stack virtual-chassis-id** command on page 82.24.

Caution

Stack operation is only supported if stack virtual-mac is enabled.
Before enabling the virtual MAC address feature, you should check that the stack's virtual-chassis-id is not already used by another stack in the network. Otherwise the duplicate MAC addresses will cause problems for the network traffic.

Syntax

```
stack virtual-mac
no stack virtual mac
```

Mode Global Configuration

Usage Note that this command will not take effect until the switch has been rebooted.

Example

```
awplus# configure terminal
awplus(config)# stack virtual mac
```

Related Commands

show running-config
show stack
switch provision (stack)
stack virtual-chassis-id

switch provision (stack)

This command enables you to provide the configuration for a new stack member switch prior to physically connecting it to the stack. To run this command, the stack position must be vacant. The selected hardware type must be compatible existing stack hardware.

Use the **no** variant of this command to remove an existing switch provision.

Syntax

```
switch <stack-ID> {provision|reprovision} {gs900-24|gs900-48}
no switch <stack-ID> provision
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 4.
provision	Provides settings within the stack configuration ready for a specific switch type to become a stack member.
reprovision	Reconfigure an existing provision configuration.
gs900-24	Provision a 24-port switch.
gs900-48	Provision a 48-port switch.

Mode

Global Configuration

Usage

Note that although the syntax appears to allow provisioning on up to 8 stackable switches, in practice a maximum of 4 are configurable. Normally the stack members would be numbered 1 to 4, and so the command could be run to provision any stack member within this range; and we advise this procedure.

However, you could number the stack units with any numbers between 1-8. For example you could number your four stack members 1, 2, 7 and 8. In this case you could provision any of the stack members within this range. We advise against numbering your stacks in this way.

Examples

To provision a GS924MPX switch as stack member 3, use the following commands:

```
awplus# configure terminal
awplus(config)# switch 3 provision gs900-24
```

To remove the provision of the switch as stack member 3, use the following commands:

```
awplus# configure terminal
awplus(config)# no switch 3 provision
```

Related Commands

show provisioning (stack)
show stack
switch provision (stack)

switchport resiliencylink

This command configures the switch port to be a member of the stack resiliency link VLAN. Note that this switchport will only be used for stack resiliency-link traffic and will not perform any other function, or carry any other traffic.

The **no** variant of this command removes the switchport from the resiliency link VLAN.

Syntax

```
switchport resiliencylink
no switchport resiliencylink
```

Mode Interface Configuration

Usage Note that a resiliency link cannot be part of a static or dynamic aggregator group.

Examples To set the resiliency link to be VLAN 4093:

First, use the **stack resiliencylink** command to create the resiliency `vlan4093`

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next, use the **switchport resiliencylink** command to assign the resiliencylink vlan to the port, in this case `port1.0.1`.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

Related Commands **stack resiliencylink**

Appendix A: Command List

A

aaa accounting auth-mac default 45.2
aaa accounting auth-web default 45.4
aaa accounting commands 45.8
aaa accounting dot1x 45.10
aaa accounting login 45.12
aaa accounting update 45.14
aaa accounting wireless 45.6
aaa authentication auth-mac 45.15
aaa authentication auth-web 45.16
aaa authentication dot1x 45.17
aaa authentication enable default group tacacs+ 45.18
aaa authentication enable default local 45.20
aaa authentication login 45.21
aaa group server 45.24
aaa local authentication attempts lockout-time 45.25
aaa local authentication attempts max-fail 45.26
accept-lifetime 31.3
access-group 37.4
access-list extended (named) 38.4
access-list hardware (named) 37.18
access-list standard (named) 38.27
access-list (extended numbered) 38.12
access-list (hardware IP numbered) 37.6
access-list (hardware MAC numbered) 37.15
access-list (standard numbered) 38.29
accounting login 45.27
activate 11.2
active (ping-polling) 80.3
active (trigger) 76.2
alliedware-behavior 31.5
arp log 25.6
arp security violation 56.3
arp security 56.2
arp (IP address MAC) 25.5
arp-aging-timeout 25.4
arp-mac-disparity 25.3
atmf backup bandwidth 61.5
atmf backup delete 61.6
atmf backup enable 61.7
atmf backup now 61.8
atmf backup server 61.10
atmf backup stop 61.12
atmf backup synchronize 61.13
atmf backup 61.4

atmf cleanup 61.14
atmf distribute firmware 61.15
atmf domain vlan 61.17
atmf enable 61.18
atmf group (membership) 61.19
atmf log-verbose 61.21
atmf management subnet 61.22
atmf management vlan 61.24
atmf master 61.26
atmf network-name 61.27
atmf provision node clone 61.29
atmf provision node configure boot config 61.31
atmf provision node configure boot system 61.32
atmf provision node create 61.33
atmf provision node delete 61.35
atmf provision node license-cert 61.37
atmf provision node locate 61.39
atmf provision 61.28
atmf reboot-rolling 61.40
atmf recover led-off 61.45
atmf recover 61.44
atmf remote-login 61.46
atmf restricted-login 61.47
atmf working-set 61.48
auth auth-fail vlan 43.3
auth critical 43.5
auth dynamic-vlan-creation 43.6
auth guest-vlan 43.9
auth host-mode 43.11
auth log 43.13
auth max-supplicant 43.15
auth reauthentication 43.16
auth roaming disconnected 43.17
auth roaming enable 43.19
auth supplicant-mac 43.21
auth timeout connect-timeout 43.23
auth timeout quiet-period 43.24
auth timeout reauth-period 43.25
auth timeout server-timeout 43.26
auth timeout supp-timeout 43.27
auth two-step enable 43.28
auth-mac enable 43.31
auth-mac method 43.32
auth-mac password 43.33
auth-mac reauth-relearning 43.34
auth-web enable 43.35
auth-web forward 43.36
auth-web max-auth-fail 43.38
auth-web method 43.39
auth-web-server blocking-mode 43.40
auth-web-server dhcp ipaddress 43.41
auth-web-server dhcp lease 43.42
auth-web-server dhcp-wpad-option 43.43
auth-web-server gateway (deleted) 43.44
auth-web-server host-name 43.45
auth-web-server http-redirect (deleted) 43.46
auth-web-server intercept-port 43.47

auth-web-server ipaddress....43.48
auth-web-server login-url....43.49
auth-web-server mode (deleted)....43.50
auth-web-server page logo....43.51
auth-web-server page sub-title....43.52
auth-web-server page success-message....43.53
auth-web-server page title....43.54
auth-web-server page welcome-message....43.55
auth-web-server ping-poll enable....43.56
auth-web-server ping-poll failcount....43.57
auth-web-server ping-poll interval....43.58
auth-web-server ping-poll reauth-timer-refresh....43.59
auth-web-server ping-poll timeout....43.60
auth-web-server port....43.61
auth-web-server redirect-delay-time....43.62
auth-web-server redirect-url....43.63
auth-web-server session-keep....43.64
auth-web-server ssl intercept-port....43.67
auth-web-server sslport (deleted)....43.66
auth-web-server ssl....43.65
autoboot enable....7.5

B

backpressure....15.2
banner exec....8.2
banner login (SSH)....54.2
banner login (system)....8.4
banner motd....8.5
boot config-file backup....7.8
boot config-file....7.6
boot system backup....7.11
boot system....7.9

C

cd....7.12
channel-group....21.3
cisco-metric-behavior (RIP)....31.7
class-map....41.3
class....41.2
clear aaa local user lockout....45.28
clear arp security statistics....56.4
clear arp-cache....25.9
clear atmf links statistics....61.49
clear counter stack....82.3
clear exception log....10.2
clear ip dhcp snooping binding....56.5
clear ip dhcp snooping statistics....56.6
clear ip igmp group....33.3
clear ip igmp interface....33.4
clear ip igmp....33.2
clear ip prefix-list....38.35
clear ip rip route....31.8
clear ipv6 mld group....35.3
clear ipv6 mld interface....35.3

clear ipv6 mld 35.2
clear ipv6 neighbors 27.2
clear lacp counters 21.5
clear line console 5.2
clear line vty 5.3
clear lldp statistics 70.2
clear lldp table 70.3
clear log buffered 10.3
clear log permanent 10.3
clear log 10.2
clear loop-protection counters 15.3
clear mac address-table dynamic 15.5
clear mac address-table static 15.4
clear mls qos interface policer-counters 41.4
clear ping-poll 80.4
clear port counter 15.7
clear power-inline counters interface 23.3
clear spanning-tree detected protocols (RSTP and MSTP) 19.4
clear spanning-tree statistics 19.3
clear ssh 54.3
clear test cable-diagnostics tdr 78.2
clear test interface 13.2
clock set 8.6
clock summer-time date 8.7
clock summer-time recurring 8.9
clock timezone 8.11
commit (IPv4) 37.35
configure terminal 4.2
copy current-software 7.12
copy debug 7.13
copy proxy-autoconfig-file 43.68
copy running-config 7.14
copy startup-config 7.15
copy web-auth-https-file 43.68
copy zmodem 7.18
copy (URL) 7.16
create autoboot 7.19
critical-interval 80.5
crypto key destroy hostkey 54.4
crypto key destroy userkey 54.5
crypto key generate hostkey 54.6
crypto key generate userkey 54.7
crypto key pubkey-chain knownhosts 54.8
crypto key pubkey-chain userkey 54.10

D

day 76.3
deadtime (RADIUS server group) 49.2
debug aaa 45.29
debug arp security 56.7
debug atmf packet 61.52
debug atmf 61.50
debug dot1x 47.2
debug epsr 58.3
debug igmp 33.5

debug ip dhcp snooping 56.8
debug ip packet interface 25.9
debug lacp 21.6
debug lldp 70.4
debug mail 71.2
debug mld 35.4
debug mstp (RSTP and STP) 19.5
debug ping-poll 80.6
debug power-inline 23.4
debug radius 49.3
debug rip 31.9
debug snmp 67.2
debug ssh client 54.12
debug ssh server 54.13
debug trigger 76.4
default log buffered 10.4
default log console 10.4
default log email 10.5
default log host 10.5
default log monitor 10.6
default log permanent 10.6
default-action 41.5
default-information originate (RIP) 31.10
default-metric (RIP) 31.11
delete debug 7.21
delete mail 71.3
delete 7.20
description (interface) 12.2
description (ping-polling) 80.7
description (QoS policy-map) 41.6
description (trigger) 76.5
devicentp master 63.6
dir 7.22
disable (Privileged Exec mode) 4.2
distance (RIP) 31.12
distribute-list (RIP) 31.13
dot1x control-direction 47.3
dot1x eapol-version 47.5
dot1x eap 47.4
dot1x initialize interface 47.6
dot1x initialize supplicant 47.7
dot1x keytransmit 47.8
dot1x max-auth-fail 47.9
dot1x max-reauth-req 47.11
dot1x port-control 47.12
dot1x timeout tx-period 47.14
do 4.3
duplex 15.8

E

echo 11.3
ecofriendly led 8.12
ecofriendly lpi 8.13
edit (URL) 7.25
edit 7.24

egress-rate-limit 41.7
enable password 5.4
enable secret 5.7
enable (Privileged Exec mode) 4.4
end 4.6
epsr configuration 58.5
epsr datavlan 58.6
epsr enhancedrecovery enable 58.7
epsr mode master controlvlan primary port 58.8
epsr mode transit controlvlan 58.9
epsr priority 58.10
epsr state 58.11
epsr trap 58.12
epsr 58.4
erase factory-default 61.55
erase proxy-autoconfig-file 43.69
erase startup-config 7.26
erase web-auth-https-file 43.69
exec-timeout 5.10
exit 4.6

F

fail-count 80.8
findme 8.15
flowcontrol hardware (asyn/console) 5.11
flowcontrol (switch port) 15.9
fullupdate (RIP) 31.14

H

help 4.7
hostname 8.17

I

instance priority (MSTP) 19.8
instance vlan (MSTP) 19.10
interface (to configure) 12.3
ip address dhcp 65.3
ip address 25.11
ip dhcp snooping agent-option allow-untrusted 56.11
ip dhcp snooping agent-option circuit-id vlantriplet 56.12
ip dhcp snooping agent-option remote-id 56.13
ip dhcp snooping agent-option 56.10
ip dhcp snooping binding 56.14
ip dhcp snooping database 56.15
ip dhcp snooping delete-by-client 56.16
ip dhcp snooping delete-by-linkdown 56.17
ip dhcp snooping max-bindings 56.18
ip dhcp snooping subscriber-id 56.19
ip dhcp snooping trust 56.20
ip dhcp snooping verify mac-address 56.21
ip dhcp snooping violation 56.22
ip dhcp snooping 56.9

ip dhcp-relay agent-option checking 65.6
ip dhcp-relay agent-option remote-id 65.7
ip dhcp-relay agent-option 65.4
ip dhcp-relay information policy 65.8
ip dhcp-relay maxhops 65.10
ip dhcp-relay max-message-length 65.11
ip dhcp-relay server-address 65.13
ip domain-list 25.13
ip domain-lookup 25.14
ip domain-name 25.15
ip gratuitous-arp-link 25.16
ip igmp snooping fast-leave 33.7
ip igmp snooping querier 33.8
ip igmp snooping report-suppression 33.9
ip igmp snooping tcn query solicit 33.10
ip igmp snooping 33.6
ip igmp static-group 33.12
ip igmp version 33.13
ip name-server 25.17
ip radius source-interface 49.4
ip rip authentication key-chain 31.15
ip rip authentication mode 31.18
ip rip authentication string 31.22
ip rip receive version 31.25
ip rip receive-packet 31.24
ip rip send version 1-compatible 31.29
ip rip send version 31.27
ip rip send-packet 31.26
ip rip split-horizon 31.30
ip route 29.3
ip rrp snooping 59.3
ip source binding 56.23
ip (ping-polling) 80.9
ipv6 access-list extended proto 39.8
ipv6 access-list extended (named) 39.4
ipv6 access-list standard (named) 39.16
ipv6 address autoconfig 27.5
ipv6 address 27.3
ipv6 enable 27.7
ipv6 forwarding 27.8
ipv6 mld access-group 35.5
ipv6 mld limit 35.6
ipv6 mld snooping fast-leave 35.10
ipv6 mld snooping mrouter 35.11
ipv6 mld snooping querier 35.13
ipv6 mld snooping report-suppression 35.14
ipv6 mld snooping 35.8
ipv6 mld static-group 35.16
ipv6 nd managed-config-flag 27.9
ipv6 nd minimum-ra-interval 27.10
ipv6 nd other-config-flag 27.11
ipv6 nd prefix 27.12
ipv6 nd ra-interval 27.14
ipv6 nd ra-lifetime 27.15
ipv6 nd reachable-time 27.16
ipv6 nd retransmission-time 27.17
ipv6 nd suppress-ra 27.18

ipv6 neighbor 27.19
ipv6 opportunistic-nd 27.20
ipv6 route 27.21

K

key chain 31.32
key-string 31.33
key 31.31

L

lacp port-priority 21.7
lacp system-priority 21.8
lacp timeout 21.9
length (asyn) 5.13
length (ping-poll data) 80.10
line 5.14
linkflap action 15.11
lldp faststart-count 70.5
lldp holdtime-multiplier 70.6
lldp management-address 70.7
lldp med-notifications 70.8
lldp med-tlv-select 70.9
lldp non-strict-med-tlv-order-check 70.11
lldp notification-interval 70.12
lldp notifications 70.13
lldp port-number-type 70.14
lldp reinit 70.15
lldp run 70.16
lldp timer 70.17
lldp tlv-select 70.18
lldp transmit receive 70.20
lldp tx-delay 70.21
location civic-location configuration 70.22
location civic-location identifier 70.26
location civic-location-id 70.27
location coord-location configuration 70.28
location coord-location identifier 70.30
location coord-location-id 70.31
location elin-location-id 70.33
location elin-location 70.32
log buffered size 10.11
log buffered (filter) 10.8
log buffered 10.7
log console (filter) 10.13
log console 10.12
log email time 10.20
log email (filter) 10.17
log email 10.16
log host time 10.26
log host (filter) 10.23
log host 10.22
log monitor (filter) 10.28
log permanent size 10.33
log permanent (filter) 10.31

log permanent 10.30
login authentication 45.30
logout 4.7
log-rate-limit nsm 10.34
loop-protection action-delay-time 15.14
loop-protection action 15.13
loop-protection timeout 15.15
loop-protection 15.12

M

mac address-table acquire 15.16
mac address-table ageing-time 15.17
mac address-table static 15.18
mac address-table thrash-limit 15.19
mail from 71.5
mail smtpserver 71.6
mail 71.4
match access-group 41.8
match cos 41.9
match dscp 41.10
match eth-format protocol 41.11
match ip-precedence 41.14
match mac-type 41.15
match tcp-flags 41.16
match vlan 41.17
max-fib-routes 8.19
maximum-access-list 38.36
maximum-paths 29.5
maximum-prefix 31.34
max-static-routes 8.20
mirror interface 15.20
mkdir 7.27
mls qos cos 41.18
mls qos enable 41.19
mls qos map cos-queue to 41.20
mls qos map premark-dscp to 41.21
move debug 7.29
move 7.28
mru 12.5
mtu 12.7

N

neighbor (RIP) 31.35
network (RIP) 31.36
no debug all 8.21
no police 41.23
normal-interval 80.11
ntp access-group 63.2
ntp authenticate 63.3
ntp authentication-key 63.4
ntp broadcastdelay 63.5

ntp peer 63.7
ntp server 63.9
ntp source 63.11
ntp trusted-key 63.13

O

offset-list (RIP) 31.37

P

passive-interface (RIP) 31.38
ping ipv6 ..... 27.22
ping-poll 80.12
ping 25.18
platform stop-unreg-mc-flooding 15.22
polarity 15.24
police single-rate action 41.24
police twin-rate action 41.26
policy-map 41.28
port-vlan-forwarding-priority 17.3
power-inline allow-legacy 23.5
power-inline description 23.6
power-inline enable 23.7
power-inline max 23.8
power-inline priority 23.10
power-inline usage-threshold 23.12
priority-queue 41.29
private-vlan association 17.7
private-vlan 17.6
privilege level 5.16
pwd 7.30

R

radius-server deadtime 49.5
radius-server host 49.6
radius-server key 49.10
radius-server retransmit 49.11
radius-server timeout 49.12
reboot rolling 82.4
reboot 8.22
recv-buffer-size (RIP) 31.39
redistribute (RIP) 31.40
region (MSTP) 19.11
reload rolling 82.4
reload 8.23
remark new-cos 41.32
remark-map 41.30
remote-login 82.5
repeat 76.6
restart rip graceful 31.41
revision (MSTP) 19.12
rip restart grace-period 31.42
rmdir 7.31

rmon alarm 73.2
rmon collection history 73.4
rmon collection stats 73.5
rmon event 73.6
route (RIP) 31.43
router rip 31.44

S

sample-size 80.13
script 76.7
security-password forced-change 5.18
security-password history 5.17
security-password lifetime 5.19
security-password minimum-categories 5.20
security-password minimum-length 5.21
security-password reject-expired-pwd 5.22
security-password warning 5.23
send-lifetime 31.45
server (Server Group) 49.14
service advanced-vty 5.24
service dhcp-relay 65.15
service dhcp-snooping 56.24
service http 5.25
service password-encryption 5.26
service power-inline 23.13
service ssh 54.14
service telnet 5.27
service test 13.3
service-policy input 41.34
show aaa local user locked 45.31
show access-list (IPv4 Hardware ACLs) 37.36
show access-list (IPv4 Software ACLs) 38.37
show arp security interface 56.27
show arp security statistics 56.28
show arp security 56.26
show arp 25.19
show atmf backup 61.60
show atmf detail 61.63
show atmf group members 61.67
show atmf group 61.65
show atmf links detail 61.70
show atmf links statistics 61.76
show atmf links 61.69
show atmf memory 61.79
show atmf nodes 61.80
show atmf provision nodes 61.81
show atmf tech 61.82
show atmf working-set 61.84
show atmf 61.56
show auth two-step supplicant brief 43.70
show auth-mac diagnostics 43.72
show auth-mac interface 43.73
show auth-mac sessionstatistics 43.76
show auth-mac statistics interface 43.77
show auth-mac supplicant interface 43.80

show auth-mac supplicant 43.78
show auth-mac 43.71
show auth-web diagnostics 43.83
show auth-web interface 43.84
show auth-web sessionstatistics 43.87
show auth-web statistics interface 43.88
show auth-web supplicant interface 43.90
show auth-web supplicant 43.89
show auth-web-server page 43.92
show auth-web-server 43.91
show auth-web 43.81
show autoboot 7.32
show banner login 54.16
show boot 7.33
show class-map 41.35
show clock 8.24
show counter dhcp-client 65.16
show counter dhcp-relay 65.17
show counter log 10.35
show counter mail 71.7
show counter ntp 63.14
show counter ping-poll 80.14
show counter snmp-server 67.4
show counter stack 82.6
show cpu history 8.28
show cpu 8.25
show crypto key hostkey 54.17
show crypto key pubkey-chain knownhosts 54.18
show crypto key pubkey-chain userkey 54.19
show crypto key userkey 54.20
show debugging aaa 45.32
show debugging arp security 56.30
show debugging atmf packet 61.86
show debugging atmf 61.85
show debugging dot1x 47.15
show debugging epsr 58.12
show debugging igmp 33.14
show debugging ip dhcp snooping 56.31
show debugging ip packet 25.20
show debugging lacp 21.11
show debugging lldp 70.34
show debugging mld 35.19
show debugging mstp 19.13
show debugging power-inline 23.14
show debugging radius 49.16
show debugging rip 31.47
show debugging snmp 67.8
show debugging trigger 76.9
show debugging 8.30
show dhcp lease 65.19
show diagnostic channel-group 21.12
show dot1x diagnostics 47.18
show dot1x interface 47.19
show dot1x sessionstatistics 47.24
show dot1x statistics interface 47.25
show dot1x supplicant interface 47.28
show dot1x supplicant 47.26

show dot1x 47.16
show ecofriendly 8.31
show epsr common segments 58.16
show epsr config-check 58.17
show epsr counters 58.19
show epsr summary 58.20
show epsr <epsr-instance> counters 58.18
show epsr <epsr-instance> 58.18
show epsr 58.13
show etherchannel detail 21.14
show etherchannel summary 21.15
show etherchannel 21.13
show exception log 10.36
show file systems 7.36
show file 7.35
show flowcontrol interface 15.25
show history 4.8
show hosts 25.21
show interface access-group 37.38
show interface brief 12.12
show interface memory 8.33
show interface status 12.13
show interface 12.9
show ip access-list 38.39
show ip dhcp snooping acl 56.33
show ip dhcp snooping agent-option 56.35
show ip dhcp snooping binding 56.36
show ip dhcp snooping interface 56.37
show ip dhcp snooping statistics 56.39
show ip dhcp snooping 56.32
show ip dhcp-relay 65.20
show ip domain-list 25.21
show ip domain-name 25.22
show ip igmp groups 33.15
show ip igmp interface 33.16
show ip igmp snooping statistics 33.19
show ip interface 25.23
show ip name-server 25.24
show ip protocols rip 31.47
show ip rip database 31.49
show ip rip interface 31.49
show ip rip 31.48
show ip route database 29.8
show ip route summary 29.9
show ip route 29.6
show ip rrp snooping 59.4
show ip sockets 25.25
show ip source binding 56.42
show ipv6 access-list (IPv6 Software ACLs) 39.20
show ipv6 forwarding 27.23
show ipv6 interface brief 27.24
show ipv6 mld groups 35.20
show ipv6 mld interface 35.21
show ipv6 mld snooping mrouter 35.22
show ipv6 mld snooping statistics 35.23
show ipv6 neighbors 27.25
show ipv6 route summary 27.28

show ipv6 route 27.26
show lacp sys-id 21.16
show lacp-counter 21.17
show lldp interface 70.37
show lldp local-info 70.39
show lldp neighbors detail 70.45
show lldp neighbors 70.43
show lldp statistics interface 70.49
show lldp statistics 70.48
show lldp 70.35
show location 70.51
show log config 10.39
show log permanent 10.42
show log 10.37
show loop-protection 15.26
show mac address-table thrash-limit 15.29
show mac address-table 15.27
show mail 71.8
show memory allocations 8.37
show memory history 8.38
show memory pools 8.40
show memory shared 8.41
show memory 8.35
show mirror interface 15.31
show mirror 15.30
show mls qos interface policer-counters 41.39
show mls qos interface queue-counters 41.40
show mls qos interface storm-status 41.41
show mls qos interface 41.37
show mls qos maps cos-queue 41.42
show mls qos maps premark-dscp 41.43
show mls qos 41.36
show ntp associations 63.15
show ntp status 63.16
show ping-poll 80.16
show platform classifier statistics utilization brief 15.33
show platform port 15.34
show platform 15.32
show policy-map 41.44
show port etherchannel 21.18
show port-security interface 15.40
show port-security intrusion 15.41
show port-vlan-forwarding-priority 17.8
show power-inline counters 23.18
show power-inline interface detail 23.22
show power-inline interface 23.20
show power-inline 23.15
show privilege 5.28
show process 8.42
show provisioning (stack) 82.10
show proxy-autoconfig-file 43.93
show radius statistics 49.19
show radius 49.17
show reboot history 8.44
show rmon alarm 73.7
show rmon event 73.8
show rmon history 73.9

show rmon statistics 73.10
show router-id 8.45
show running-config access-list 7.40
show running-config as-path access-list 7.41
show running-config atmf 61.87
show running-config dhcp 7.42
show running-config full 7.43
show running-config interface 7.44
show running-config ip route 7.46
show running-config ipv6 access-list 7.47
show running-config ipv6 route 7.48
show running-config key chain 7.49
show running-config lldp 7.50
show running-config log 10.43
show running-config power-inline 7.51
show running-config route-map 7.52
show running-config router-id 7.54
show running-config router 7.53
show running-config security-password 7.55
show running-config snmp 67.8
show running-config ssh 54.21
show running-config trigger 76.9
show running-config 7.38
show security-password configuration 5.29
show security-password user 5.30
show snmp-server community 67.9
show snmp-server group 67.10
show snmp-server user 67.10
show snmp-server view 67.11
show snmp-server 67.9
show spanning-tree brief 19.17
show spanning-tree mst config 19.19
show spanning-tree mst detail interface 19.22
show spanning-tree mst detail interface 19.27
show spanning-tree mst detail 19.20
show spanning-tree mst instance interface 19.25
show spanning-tree mst instance 19.24
show spanning-tree mst interface 19.26
show spanning-tree mst 19.18
show spanning-tree statistics instance interface 19.31
show spanning-tree statistics instance 19.30
show spanning-tree statistics interface 19.32
show spanning-tree statistics 19.29
show spanning-tree vlan range-index 19.34
show spanning-tree 19.14
show ssh client 54.23
show ssh server allow-users 54.25
show ssh server deny-users 54.26
show ssh server 54.24
show ssh 54.22
show stack 82.11
show startup-config 7.56
show static-channel-group 21.19
show storm-control 15.42
show system environment 8.47
show system interrupts 8.48
show system mac 8.49

show system pci device 8.50
show system pci tree 8.51
show system pluggable detail 8.55
show system pluggable diagnostics 8.59
show system pluggable 8.52
show system serialnumber 8.62
show system 8.46
show tacacs+ 51.3
show tech-support 8.63
show telnet 5.31
show test cable-diagnostics tdr 78.3
show trigger 76.10
show users 5.32
show version 7.57
show vlan classifier group interface 17.11
show vlan classifier group 17.10
show vlan classifier interface group 17.12
show vlan classifier rule 17.13
show vlan 17.9
shutdown 12.15
snmp trap link-status suppress 67.13
snmp trap link-status 67.12
snmp-server community 67.16
snmp-server contact 67.17
snmp-server enable trap 67.18
snmp-server engineID local reset 67.22
snmp-server engineID local 67.20
snmp-server group 67.23
snmp-server host 67.24
snmp-server location 67.26
snmp-server source-interface 67.27
snmp-server startup-trap-delay 67.28
snmp-server user 67.29
snmp-server view 67.31
snmp-server 67.15
source-ip 80.20
spanning-tree autoedge (RSTP and MSTP) 19.35
spanning-tree bpdu 19.36
spanning-tree cisco-interoperability (MSTP) 19.38
spanning-tree edgeport (RSTP and MSTP) 19.39
spanning-tree enable 19.40
spanning-tree errdisable-timeout enable 19.42
spanning-tree errdisable-timeout interval 19.43
spanning-tree force-version 19.44
spanning-tree forward-time 19.45
spanning-tree guard root 19.46
spanning-tree hello-time 19.47
spanning-tree link-type 19.48
spanning-tree max-age 19.49
spanning-tree max-hops (MSTP) 19.50
spanning-tree mode 19.51
spanning-tree mst configuration 19.52
spanning-tree mst instance path-cost 19.54
spanning-tree mst instance priority 19.56
spanning-tree mst instance restricted-role 19.57
spanning-tree mst instance restricted-tcn 19.58
spanning-tree mst instance 19.53

spanning-tree path-cost 19.59
spanning-tree portfast bpdu-filter 19.62
spanning-tree portfast bpdu-guard 19.64
spanning-tree portfast (STP) 19.60
spanning-tree priority (bridge priority) 19.66
spanning-tree priority (port priority) 19.67
spanning-tree restricted-role 19.68
spanning-tree restricted-tcn 19.68
spanning-tree transmit-holdcount 19.69
speed (asyn) 8.66
speed 15.43
ssh client 54.29
ssh server allow-users 54.33
ssh server authentication 54.35
ssh server deny-users 54.37
ssh server resolve-host 54.38
ssh server scp 54.39
ssh server sftp 54.40
ssh server 54.31
ssh 54.27
stack disabled-master-monitoring 82.15
stack enable 82.16
stack management subnet 82.17
stack management vlan 82.18
stack priority 82.19
stack renumber cascade 82.21
stack renumber 82.20
stack resiliencylink 82.22
stack virtual-chassis-id 82.24
stack virtual-mac 82.25
static-channel-group 21.20
storm-action 41.45
storm-control level 15.45
storm-downtime 41.46
storm-protection 41.47
storm-rate 41.48
storm-window 41.49
switch provision (stack) 82.26
switchport access vlan 17.14
switchport atmf-link 61.88
switchport enable vlan 17.15
switchport mode access 17.16
switchport mode private-vlan trunk promiscuous 17.18
switchport mode private-vlan trunk secondary 17.20
switchport mode private-vlan 17.17
switchport mode trunk 17.22
switchport private-vlan host-association 17.23
switchport private-vlan mapping 17.24
switchport resiliencylink 82.27
switchport trunk allowed vlan 17.25
switchport trunk native vlan 17.28
switchport voice dscp 17.29
switchport voice vlan priority 17.32
switchport voice vlan 17.30
system territory (deprecated) 8.68

T

tacacs-server host 51.4
tacacs-server key 51.7
tacacs-server timeout 51.8
tcpdump 25.27
telnet server 5.34
telnet 5.33
terminal length 5.35
terminal monitor 8.69
terminal resize 5.36
test cable-diagnostics tdr interface 78.4
test interface 13.4
test 76.15
thrash-limiting 15.46
time (trigger) 76.16
timeout (ping polling) 80.21
timers (RIP) 31.50
traceroute ipv6 ..... 27.29
traceroute 25.28
trap 76.18
trigger activate 76.20
trigger 76.19
trust dscp 41.50
type atmf node 61.89
type atmf node 76.21
type cpu 76.23
type interface 76.24
type memory 76.25
type periodic 76.26
type ping-poll 76.27
type reboot 76.27
type stack disabled-master 76.28
type stack link 76.29
type stack master-fail 76.30
type stack member 76.31
type time 76.32
type usb 76.33

U

undebug aaa 45.32
undebug all 8.70
undebug dot1x 47.31
undebug epsr 58.20
undebug igmp 33.20
undebug lacp 21.22
undebug mail 71.8
undebug mstp 19.69
undebug ping-poll 80.22
undebug radius 49.19
undebug rip 31.51
undebug snmp 67.32
undebug ssh client 54.41
undebug ssh server 54.41
undebug trigger 76.33

up-count 80.22
username 5.37

V

version 31.52
vlan classifier activate 17.34
vlan classifier group 17.35
vlan classifier rule ipv4 ..... 17.36
vlan classifier rule proto 17.37
vlan database 17.40
vlan 17.33

W

wait 11.4
write file 7.58
write memory 7.58
write terminal 7.58
wrr-queue disable queues 41.51
wrr-queue weight queues 41.52

Z

(access-list extended ICMP filter) 38.15
(access-list extended IP filter) 38.17
(access-list extended IP protocol filter) 38.20
(access-list extended TCP UDP filter) 38.24
(access-list hardware ICMP filter) 37.20
(access-list hardware IP protocol filter) 37.23
(access-list hardware MAC filter) 37.29
(access-list hardware TCP UDP filter) 37.32
(access-list standard named filter) 38.31
(access-list standard numbered filter) 38.33
(ipv6 access-list extended IP protocol filter) 39.11
(ipv6 access-list extended TCP UDP filter) 39.14
(ipv6 access-list standard filter) 39.18

Appendix B: Glossary

Numerics B.2
A B.2
B B.5
C B.6
D B.8
E B.10
F B.11
G B.12
H B.12
I B.12
L B.14
M B.16
N B.18
P B.18
Q B.20
R B.21
S B.23
T B.26
U B.27
V B.28
W B.29

Numerics

10BaseT

10 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.

802.1X

IEEE 802.1x is an IEEE Standard for port-based Network Access Control (**NAC**). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for securing wireless 802.11 access points and is based on the Extensible Authentication Protocol (**EAP**). Authentication is required on a per-port basis. The main components of an 802.1X implementation are:

- The authenticator - the port on this device that wishes to enforce authentication before allowing access to services that are accessible behind it.
- The supplicant - the port that wishes to access services offered by the authenticator's system. The supplicant may be a port on a PC or other device connected to this device.
- The authentication server - a device that uses the authentication credentials supplied by the supplicant, via the authenticator, to determine if the authenticator should grant access to its services.

See **AAA** and **Tri-authentication**.

For a configuration example see **"Configuring 802.1X" on page 46.6**. For a sample configuration script see **"Sample 802.1X-Authentication Configuration" on page 44.7**.

A

AAA

AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These function can be applied in a variety of methods with a variety of servers.

Authentication is performed in the following contexts:

- Login authentication of user shell sessions on the console port, and via telnet/SSH.
- **802.1X** authentication of devices connecting to switch ports.
- **MAC authentication** of devices connecting to switch ports.
- **Web-authentication** of devices connecting to switch ports.

Accounting is performed in the following contexts:

- Accounting of console login sessions.
- Accounting of 802.1x authenticated connections.
- Accounting of MAC authenticated connections.
- Accounting of Web authenticated connections.

There are two types of servers that can be used:

- Local user database.
- **RADIUS** servers.

When 802.1X authentication, MAC authentication and Web-authentication are configured to run simultaneously on a switch port this is called tri-authentication.

For more information see **Chapter 44, AAA Introduction and Configuration**. For a configuration example see **"Configuring AAA Login Authentication" on page 44.5**. For sample 802.1x, MAC authentication and Web-authentication configuration scripts see **"Sample Authentication Configurations" on page 44.7**.

Access-list

See **ACL**.

ACL

Access Control List. An ACL is one filter, or a sequence of filters, that are applied to an interface to either block, pass, or when using QoS, apply priority to, packets that match the filter definitions. ACLs are used to restrict network access by hosts and devices and to limit network traffic. See **ACL sequence numbers** and **ACL types**.

For more information see **Chapter 36, Access Control Lists Introduction**.

ACL sequence numbers

To help manage **ACLs** you can apply sequence numbers to filters. This allows you to remove filters from named and numbered ACLs without having to reconfigure an ACL. The ability to add sequence numbers to filters simplifies updates through the ability to position a filter within an ACL. When you add a new filter, you can specify a sequence number to position the filter in the ACL and you can also remove a current filter in an ACL by specifying a sequence number.

For more information see **"ACL Filter Sequence Numbers" on page 36.14**.

ACL types

ACLs are separated into two different types, software ACLs and hardware ACLs.

Hardware ACLs are applied directly to an interface, or are used for QoS **Classifications**. They can be either named, or can use the following numeric ranges:

- 3000-3699 for Hardware IP ACLs
- 4000-4699 for Hardware MAC ACLs

For more information see **"Defining Hardware IP ACLs" on page 36.6** and **"Defining Hardware MAC ACLs" on page 36.5**.

Software ACLs can be either named ACLs, using the standard or extended keyword followed by a text string, or they can use the following numeric ranges:

- 1-99
- 100-199
- 1300-1999
- 2000-2699

Software ACLs are used in features such as SNMP, IGMP, BGP and OSPF.

Active master

The switch that manages the stack, or **VCStack**, also referred to as the **Stack master**.

See **Disabled master** for information about how this relates to **Stack master** or **Active master**.

Address resolution

The process of resolving and mapping hardware MAC addresses into their corresponding network layer IP addresses. Depending on the underlying network, address resolution may require broadcasts on a local network.

For more information see **"ARP" on page B.4**.

Adjacency

A state existing between two OSPF routers. These routers build their routing databases by exchanging link state advertisements, often termed hello messages. When a pair has completed the process, the routers are said to be "adjacent."

AMF (also shown as ATMF in commands and output)

AMF (Allied Telesis Management Framework) is a suite of features that combine to simplify network management across all supported network switches from the core to the edge. Its major features are:

- Unified Command Line
- Configuration Backup and Recovery
- Rolling-Reboot Upgrade
- Node Provisioning

For more information see **"AMF Introduction and Configuration" on page 60.1**.

ARP

Address Resolution Protocol. ARP is used by your device to dynamically learn the Layer 2 address of devices in its networks. Most hosts also have a MAC physical address in addition to the assigned IP address. For Ethernet, this is a 6-byte, globally unique number. ARP enables your device to learn the physical address of the host that has a given IP address.

For more information see **"Address Resolution Protocol (ARP)" on page 24.3**.

ASCII

The *American Standard Code for Information Interchange*. A standard character-to-number encoding widely used within the computer industry.

ASIC

Application Specific Integrated Circuit. An integrated circuit (chip) manufactured to perform a specific function.

Asynchronous

Transmission in which each character is sent individually. The time intervals between transmitted characters may be of unequal length. Transmission is controlled by start and stop elements before and after each character. See **"Synchronous" on page B.26**

Autonegotiation

Autonegotiation lets the port adjust its speed and duplex mode to accommodate the device connected to it. When the port connects to another autonegotiating device, they negotiate the highest possible speed and **Duplex mode** for both of them.

B

BIST

Built In Self Test. A mechanism that permits the device to test itself.

B-MAC

Backbone MAC address.

BPDU

Bridge Protocol Data Unit. A **Spanning tree** protocol initializing packet sent at configurable intervals to exchange information among bridges in the LAN.

For information on the standardized format for MSTP BPDU messages see **"MSTP Bridge Protocol Data Units (BPDUs)" on page 18.17**.

Bridge

A device that connects two or more networks and forwards packets between them. Bridges function at the data link layer or Layer 2 of the OSI reference model. A bridge will filter, send or flood an incoming frame, base on the MAC address of that frame.

Broadcast

One device sends out data that is intended to be received and processed by every device that it reaches.

Broadcast domain

A section of an Ethernet network comprising all the devices that will receive broadcast packets sent by any device in the domain. Separated from the rest of the network by a Layer 3 switch.

BOOTP

Bootstrap Protocol. BOOTP is a UDP-based protocol that enables a booting host to dynamically configure itself without external interventions. A BOOTP server responds to requests from BOOTP clients for configuration information, such as the IP address the client should use.

B-TAG

Backbone TAG Field.

B-VID

Backbone VLAN ID (tunnel).

B-VLAN

Backbone VLAN (tunnel).

C

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication method used by PPP servers to validate the identity of clients. CHAP verifies the identity of the client by using a three-way handshake, and the verification is based on a shared secret by the client and the server, such as the client's password.

CIST

Common and Internal Spanning Tree. The CIST is the default spanning tree instance of **MSTP**, i.e. all VLANs that are not members of particular **MSTIs** are members of the CIST. Also, an individual MST region can be regarded as a single virtual bridge by other MST regions. The spanning tree that runs between regions is the CIST. The CIST is also the spanning tree that runs between MST regions and Single Spanning Tree (SST) entities.

For more information see **"Common and Internal Spanning Tree (CIST)" on page 18.15**.

Classification

In **ACLs** and **QoS**, classification is the process of filtering and marking. Filtering involves sorting your data into appropriate traffic types. Marking involves tagging the data so that downstream ports and routers can apply appropriate service policy rules. There are two reasons to classify data:

- To provide network security (security ACLs).
- To apply service quality criteria QoS.

The main application of security ACLs is to block undesired traffic. When using ACLs though QoS, the same classification and action abilities are available, but QoS has some additional fields that it can match on and also provides the ability to perform metering, marking and remarking on packets that match the filter definitions.

For more information on QoS classification see **"Classifying Your Data" on page 40.7**.

Class maps

Class maps are among the pivotal **QoS** components. They provide the means that associate the classified traffic with its appropriate QoS actions. They are the linking elements for the following functions:

- **Classification**.
- policy mapping. See **Policy maps**.
- **Premarking**.

The relationship between a class map and a policy map can be one-to-one or many-to-one.

For more information see **"Class Maps" on page 40.7**.

CLI

Command Line Interface. With three distinct modes, the CLI is very secure. In User exec mode you can view settings and troubleshoot problems but you cannot make changes to the system. In Privileged exec mode you can change system settings and restart the device. You can only make configuration changes in Global configuration mode, which reduces the risk of making accidental configuration changes.

For more information see **"How to Work with Command Modes" on page 1.7**.

C-MAC

Customer MAC Address.

Collision domain

A physical region of a local area network (LAN) in which data collisions can occur.

Control VLAN

In **EPSR**, the VLAN over which all control messages are sent and received. EPSR never blocks this VLAN.

For more information see **"Ring Components and Operation" on page 57.2**.

CoS

Class of Service. CoS is a method for classifying traffic on a packet by packet basis using information in the type-of-service (ToS) byte to provide different service levels to different traffic. See **QoS**.

For more information see **"CoS to Egress Queue Premarking" on page 40.11**.

Cost

An indication of the overhead required to send packets across a certain interface.

C-TAG

Customer VLAN TAG.

C-VID

Customer VLAN ID.

C-VLAN

Customer VLAN.

D

Data VLAN

In **EPSR**, a VLAN that needs to be protected from loops. Each EPSR domain has one or more data VLANs.

For more information see **"Ring Components and Operation" on page 57.2**.

Designated bridge

Each bridge or LAN in the **Spanning tree**, except the **Root bridge**, has a unique parent, known as the designated bridge. Each LAN has a single bridge, called the designated bridge, that connects it to the next LAN on the path towards the root bridge.

For an overview of spanning tree operation see **"Spanning Tree Operation" on page 18.2**.

DHCP

Dynamic Host Configuration Protocol. A method of automatically allocating IP addresses. A DHCP server holds a pool of IP addresses from which it draws individual ones as it allocates them to users when they log on.

For more information see **Chapter 64, Dynamic Host Configuration Protocol (DHCP) Introduction**.

DHCP relay agent option 82

Enabling the DCHP Relay Agent Option 82 feature on the switch allows the switch to insert extra information into the DHCP packets that it is relaying. The information is stored in a specific optional field in the DHCP packet, namely, the agent-information field, which has option ID 82.

Note that the DHCP Relay Agent Option 82 agent information inserted by the DHCP snooping differs from the information added by DHCP Relay. The switch cannot be configured to use both the DHCP relay agent option and DHCP snooping.

For information about the DHCP Relay Agent Option 82 information inserted by DHCP snooping see **"DHCP Relay Agent Option 82" on page 55.4**.

DHCP snooping

DHCP snooping provides an extra layer of security on the switch via dynamic IP source filtering. DHCP snooping filters out traffic received from unknown, or 'untrusted' ports, and builds and maintains a DHCP snooping database.

With DHCP snooping, IP sources are dynamically verified, and filtered accordingly. IP packets that are not sourced from recognized IP addresses can be filtered out. This ensures the required traceability.

For more information see **Chapter 55, DHCP Snooping Introduction and Configuration**. For a configuration example see **"Configure DHCP Snooping" on page 55.10**.

Digital Diagnostics Monitoring (DDM)

Modern optical SFP transceivers support Digital Diagnostics Monitoring (DDM) functions. This feature allows you to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. Additionally, RX LOS (Loss of Signal) is shown when the received optical level is below a preset threshold. Monitoring these parameters allows you to check on the health of all installed SFPs or a specific SFP transceiver. See also **Trouble-shoot Fiber and Pluggable Issues** in **Getting Started**.

SFP transceivers that support DDM display the following output from the **show system pluggable detail** and the **show system pluggable diagnostics** commands for monitoring SFPs:

- **Diagnostic Calibration**: Specifies whether the pluggable supports DDM Internal Calibration. **Internal** is displayed if the pluggable supports DDM Internal Calibration.
- **Power Monitoring**: Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in µW.

For further information about the DDM feature on the switch for installed SFP transceivers, see the **show system pluggable detail** command and the **show system pluggable diagnostics** command in **Chapter 8, System Configuration and Monitoring Commands**.

Disabled master

The Disabled Master is a variant of the **Stack master** or **Active master** and is used with the **DMM (disabled master monitoring)**feature. The Disabled Master has the same configuration as the **Stack master** or **Active master**, but has all its switchports disabled. The Disabled Master is only used is the stack separates into two stubs. By having all switchports disabled, the Disabled Master avoids potentially detrimental network connectivity problems from having two Stack Masters or Active Masters having the same configuration. The Stack Master's or Active Master's ports are unaffected by the Disabled Master's ports, so the Stack Master or Active Master continues to forward traffic normally.

For information about the Disabled Master and the Disabled Master Monitoring feature, see the **Disabled Master Monitoring (DMM)** section in **Chapter 81, VCStack Introduction** and the **stack disabled-master-monitoring** command in **Chapter 82, Stacking Commands**.

DLF

Destination Lookup Failure. DLF is the event of receiving a unicast Ethernet frame with an unknown destination address.

DMM (disabled master monitoring)

The Disabled Master Monitoring (DMM) features checks the status of the Active Master via the Stack Resiliency Link. If the Active Master fails then the Disabled Master changes state to Active Master. A Disabled Master has the same configuration as the Active Master, but has all links shutdown. This change in state for the Disabled Master to become the Active Master allows traffic forwarding to continue on the VCStack.

For information about the Disabled Master and the Disabled Master Monitoring feature, see the **Disabled Master Monitoring (DMM)** section in **Chapter 81, VCStack Introduction** and the **stack disabled-master-monitoring**

DNS

Domain Name System. DNS allows you to access remote systems by entering human-readable device host names rather than IP addresses. DNS works by creating a mapping between a device name, such as **www.alliedtelesis.com**, and its IP address. These mappings are held on DNS servers. The benefits of DNS are that domain names:

- Can map to a new IP address if the host's IP address changes.
- Are easier to remember than an IP address.
- Allow organizations to use a domain name hierarchy that is independent of any IP address assignment.

For more information see **"DNS Client" on page 24.6**.

DoS

Denial of Service. A generic term for attacks that reduce or stop the operation of a network.

DSCP value

The Differentiated Services Code Point within the TOS field of an IP packet header. This is a 6-bit number in the range 0-63.

Duplex mode

See **Full duplex** and **Half duplex**.

Dynamic channel group

A dynamic channel group also known as a LACP channel group, an etherchannel, or a LACP aggregator, enables a number of ports to be dynamically combined to form a single higher bandwidth logical connection. See **LACP**.

For an more information see **"Link Aggregation Control Protocol (LACP)" on page 20.3**. For a configuration example see **"Configuring an LACP Channel Group" on page 20.5**.

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.

E

EAP

Extensible Authentication Protocol. EAP carries out the authentication exchange between the supplicant and the authentication server.

EEE

The IEEE 802.3az Energy Efficient Ethernet (EEE) standard is a specification for lowering the power consumption of Ethernet devices during periods of low link utilization. If no data is being sent then the Ethernet device can enter a sleep state, called Low Power Idle (LPI), to conserve the power consumed by the Ethernet device. See the **LPI** glossary entry.

Etherchannel

See **Dynamic channel group**.

Ethernet Protection Switching Ring

See **EPSR**.

EPSR

EPSR (Ethernet Protection Switching Ring) operates on physical rings of switches (note, not on meshed networks). When all nodes and links in the ring are up, EPSR prevents a loop by blocking data transmission across one port. When a node or link fails, EPSR detects the failure rapidly and responds by unblocking the blocked port so that data can flow around the ring. The EPSR components are:

- **EPSR domain**
- **Master node**
- **Transit node**
- **Ring port**
- **Primary port**
- **Secondary port**
- **Control VLAN**
- **Data VLAN**

For more information and example configurations see **Chapter 57, EPSR Introduction and Configuration**.

EPSR domain

A protection scheme for an Ethernet ring that consists of one or more data VLANs and a control VLAN.

For more information see **"Ring Components and Operation" on page 57.2**.

Egress

Outgoing packet process.

F

FDB

Forwarding Database.

FIB

Forwarding Information Base. The **RIB** (Routing Information Base) populates the FIB with the best route to each destination. When your device receives an IP packet, and no filters are active that would exclude the packet, it uses the FIB to find the most specific route to the destination. If your device does not find a direct route to the destination, and no default route exists, it discards the packet and sends an ICMP message to that effect back to the source.

For more information see **"RIB and FIB Routing Tables" on page 28.4**.

Full duplex

When a port is in full duplex mode, the port transmits and receives data simultaneously. See **Half duplex**.

G

Guest VLAN

If **802.1X** authentication has been configured on access ports in the network, you might still want to provide limited network access to those users whose devices do not have 802.1x supplicant enabled, or who have unrecognized authentication credentials. The mechanism to achieve this is known as a Guest VLAN. The idea is that if the users device fails 802.1X authentication, or is not even performing any 802.1X authentication, then its connection port can be put into the guest VLAN.

For more information see **"Configuring a Guest VLAN" on page 2** and the **auth guest-vlan** command on page 43.9. For a configuration example see **"Configuring a Guest VLAN" on page 42.2**.

H

Half duplex

When a port is in half duplex mode, the port transmits or receives but not both at the same time. See **Full duplex**.

Hardware ACLs

See **ACL types**.

I

ICMP

Internet Control Message Protocol. ICMP allows networking devices to send information and control messages to other devices or hosts.

For more information see **"Internet Control Message Protocol (ICMP)" on page 24.8**.

ICMPv6

Internet Control Message Protocol Version 6. ICMPv6 is an implementation of **ICMP** for IPv6.

For more information see **"The Internet Control Message Protocol (ICMPv6)" on page 26.7**.

IGMP

Internet Group Management Protocol. IGMP is a communications protocol that hosts use to indicate that they are interested in receiving a particular multicast stream.

IGMP querier or router

A device in a subnetwork that is the coordinator for all multicast streams and IGMP membership information. Each subnet only has one active querier.

IGMP snooper

A device that spies on IGMP messages to create flow efficiencies by ensuring that multicast data streams are only sent to interested ports. A snooper can decide on the best path to send multicast packets at Layer 2 but does not initiate any IGMP communications.

For a configuration example see **"IGMP Snooping and Querier Configuration Example" on page 32.6**.

Ingress

Incoming packet process.

IP directed broadcast

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a switch that is directly connected to its destination subnet, the packet is flooded as a broadcast on the destination subnet. IP directed broadcast is enabled and disabled per VLAN interface. When enabled a directed broadcast packet is forwarded to an enabled VLAN interface if received on another subnet.

IP Helper

The IP Helper feature allows the switch to receive UDP broadcasts on one subnet, and forward them as broadcasts or unicasts into another subnet, so a client can use an application which uses UDP broadcast (such as Net-BIOS) when the client and server are located in different subnets. The IP Helper feature forwards UDP broadcast network traffic to specific hosts on another subnet and/or to the broadcast address of another subnet. When the IP Helper feature is enabled on a VLAN interface, the UDP broadcast packets received on the interface are processed for forwarding out through another interface into another subnet.

I-SID

Extended Service ID.

ISP

Internet Service Provider. An organization that offers its customers access to the Internet. The ISP connects its customers using a data transmission technology, such as dial-up or DSL.

I-TAG

Extended Service TAG.

L

LACP

Link Aggregation Control Protocol. LACP allows bundling of several physical ports to form a single logical channel providing enhanced performance and redundancy. The aggregated channel is viewed as a single link to each switch. The spanning tree views the channel as one interface and not as multiple interfaces. When there is a failure in one physical port, the other ports stay up and there is no disruption. LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).

For an more information see **"Link Aggregation Control Protocol (LACP)" on page 20.3**.

LACP aggregator

See **Dynamic channel group**.

LACP channel group

See **Dynamic channel group**.

LAG

See **Link aggregation group**.

Layer 3 switch

A Layer 3 switch is an optimized combination of routing software and specialized hardware. The software uses traditional methods (static routing commands, and routing protocols) to build up a table of the best routes to network destinations, and then writes them into a set of registers in the specialized forwarding hardware. The hardware then forwards packets, based on their Layer 3 address content, at very high data rates, using the values that are written into the registers.

LED

Light Emitting Diode (LED). An LED is a semiconductor that emits light by converting electrical energy. Power lights on switches and status lights on switch ports are LEDs. You can save power used by switch LEDs with the **ecofriendly led** command on page 8.12.

For more information and configuration examples see the section **"Save Power with the Eco-Friendly Feature" on page 1.32**. For command information and examples see the **ecofriendly led** command on page 8.12.

See also the **LPI** glossary entry.

Link aggregation group

A Link Aggregation Group is a collection of bundled switch ports for an aggregated link. Link aggregation is the bonding together of two or more data channels into a single channel that appears as single logical link of higher bandwidth increasing link performance and reliability.

For an more information see **"Link Aggregation Control Protocol (LACP)" on page 20.3**. For a configuration example see **"Configuring an LACP Channel Group" on page 20.5**

Link-local addresses

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires a link-local address is assigned to each interface, which has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the **ipv6 enable** command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

LLDP

Link Layer Discovery Protocol. LLDP is a Layer 2 protocol that enables Ethernet network devices, such as switches and routers, to transmit and/or receive device-related information to or from directly connected devices on the network, and to store such information learned about other devices. LLDP is a link level ("one hop") protocol; LLDP information can only be sent to and received from devices that are directly connected to each other, or connected via a hub or repeater. Advertised information is not forwarded on to other devices on the network.

For more information see **Chapter 69, LLDP, LLDP-MED and Voice VLAN Introduction and Configuration**.

For configuration examples see **"Configuring LLDP" on page 69.11**.

LLDPDU

LLDP Data Unit. See **LLDP advertisements**.

LLDP advertisements

LLDP transmits advertisements as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (**TLV**), each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED

Link Layer Discovery Protocol Media Endpoint Discovery. LLDP-MED is an enhancement to IEEE's 802.1AB LLDP, adding media and IP telephony-specific messages that can be exchanged between the network and endpoint devices.

For more information see **"LLDP-MED" on page 69.3**, **"LLDP-MED: Location Identification TLV" on page 69.7** and **"LLDP-MED Operation" on page 69.9**. For the procedure to configure LLDP-MED see **"Configure LLDP-MED" on page 69.14**.

LPI

Low Power Idle (LPI). LPI is a feature of the IEEE 802.3az Energy Efficient Ethernet (EEE) standard. LPI lowers power consumption of switch ports during periods of low link utilization when connected to IEEE 802.3az compliant host devices. If no data is sent then the switch port can enter a sleep state, called Low Power Idle (LPI), to conserve power used by the switch.

For more information and configuration examples see the section **Save Power with the Eco-Friendly Feature** command on page 1.32. For command information and examples see the **ecofriendly lpi** command on page 8.13. See also the **LED** glossary entry.

LSA

Link State Advertisement. OSPF sends link-state advertisements (LSAs) to all other routers within the same hierarchical area. Data on attached interfaces, metrics used, and other variables, are included in OSPF LSAs. As OSPF routers accumulate link-state data, they use the Shortest Path First (SPF) algorithm to calculate the shortest path to each node.

M

MAC address learning

A key optimization in Ethernet switching is that the flooding of unicast traffic is minimized. This is based on switches knowing which port to forward traffic to for given destination MAC addresses. Switches achieve this by the simple process of noting on which ports packets arrive from given MAC addresses, as those will be the ports to which return packets to those MAC addresses will need to be forwarded. This process is referred to as MAC address learning.

MAC authentication

The way that MAC-based authentication works is that when the supplicant device starts sending packets, the authenticating switch will extract the source MAC address from the packets, and send a RADIUS request that uses this MAC address as the username and password in the request. See **AAA** and **Tri-authentication**.

For a sample configuration script see **"Sample MAC-Authentication Configuration" on page 44.8**.

Master node

In **EPSR**, the controlling node for a domain, responsible for polling the ring state, collecting error messages, and controlling the flow of traffic in the domain.

Master node states are:

- Complete - the state when there are no link or node failures on the ring.
- Failed - the state when there is a link or node failure on the ring. This state indicates that the master node received a Link-Down message or that the failover timer expired before the master node's secondary port received a Health message.

For more information see **"Ring Components and Operation" on page 57.2**.

MD5

Message Digest 5 authentication algorithm.

Metering

See **Policing**.

Metric

The sum of all the costs along the path to a given destination. See **Cost**.

MLD

Multicast Listener Discovery. MLD is used to exchange membership status information between IPv6 routers that support multicasting and members of multicast groups on a network segment. Host membership in a multicast group is reported by individual member hosts, and membership status is periodically polled by multicast routers.

MLD snooping

MLD snooping is a feature whereby a Layer 2 switch listens to or "snoops" the MLD messages passing through the switch or from member hosts and multicast routers. The purpose of MLD snooping is to provide efficient Layer 2 multicast forwarding, by sending only to hosts that have expressed an interest in receiving the multicast data.

For more information see **Chapter 35, MLD Snooping Commands**.

MSTI

Multiple Spanning Tree Instance. **MSTP** enables the grouping and mapping of VLANs to different spanning tree instances. An MST Instance (MSTI) is a particular set of VLANs that are all using the same spanning tree.

For more information see **"Multiple Spanning Tree Instances (MSTI)" on page 18.12**.

MSTP

Multiple Spanning Tree Protocol. MSTP is similar to Rapid Spanning Tree Protocol (**RSTP**) - it provides loop resolution and rapid convergence. However it also has the extra advantage of making it possible to have different forwarding paths for different multiple spanning tree instances. This enables load balancing of network traffic across redundant links. A device running MSTP is compatible with other devices running RSTP or **STP**.

For more information see **"Multiple Spanning Tree Protocol (MSTP)" on page 18.11**. For a configuration example see **"Configuring MSTP" on page 18.19**.

MSTP regions

An MST region is a set of interconnected switches that all have the same values for the following MST configuration identification elements:

- MST configuration name - the name of the MST region.
- Revision level - the revision number of configuration.
- Configuration Digest - the mapping of which VLANs are mapped to which MST instances.

Each of the MST instances created are identified by an **MSTI** number. This number is locally significant within the MST region. Therefore, an MSTI will not span across MST regions.

For more information see **"MSTP Regions" on page 18.13**.

Multicast

One device sends out data that is intended to be received and processed by a selected group of the devices it reaches.

N

NAC

Network Access Control. NAC provides unprecedented control over user access to the network in order to mitigate threats to network infrastructure. NAC uses **802.1X** port-based authentication with standards-compliant dynamic VLAN assignment, to assess a user's adherence to the network's security policies, and either grant authentication or offer remediation. NAC also 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. Furthermore, if multiple users share a port then multi-authentication can be used and a **Guest VLAN** can be configured to provide a catch-all for users without an 802.1x supplicant.

For more information see **Chapter 46, 802.1X Introduction and Configuration** and **Chapter 42, Authentication Introduction and Configuration**.

NAS

Network Access Server. A NAS is a single point of access to a remote resource. The client connects to the NAS. The NAS then connects to another resource asking whether the client's supplied credentials are valid. Based on that answer the NAS then allows or disallows access to the resource. The NAS contains no information about what resources clients can connect to or what client credentials are valid. The NAS sends the credentials the client supplied to a resource which then validates the client.

Next hop

IP routing involves forwarding packets from one router to the next, until they reach their destination. Routers do not need to know the full path to a packet's destination, they just need to know the next router to forward the packet on to. This 'next router' is referred to as the next hop of an IP route.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the time clocks on a collection of network devices using a distributed client/server mechanism.

For more information see **Chapter 62, NTP Introduction and Configuration**.

P

PAP

Password Authentication Protocol. PAP is an authentication protocol that uses a password and is used by PPP to validate users before allowing them to access server resources. PAP transmits plain text ASCII passwords over the network so it is not secure.

PDs

Powered Devices. PDs are devices such as IP phones, wireless LAN Access Points, and network cameras. PDs receive power, in addition to data, over existing network infrastructure and cabling. See **PoE**.

Ping

Ping tests the connectivity between two network devices to determine whether each network device can "see" the other device.

Ping-of-death attack

A type of attack on a computer that involves sending a malformed or otherwise malicious ping to a network device.

Ping polling

Ping polling is used to ensure that a device is still present, live, and contactable in the network by periodically sending a packet to an IP address and waiting for a response. Configurable actions can be performed if responses are no longer arriving.

For more information see **Chapter 79, Ping Polling Introduction and Configuration**. For how to configure ping polling see **"Configuring Ping Polling" on page 79.4**.

PoE

Power over Ethernet. PoE is a mechanism for supplying power to network devices over the same cabling used to carry network traffic. PoE supplies power to network devices called Powered Devices (**PDs**).

For more information see **Chapter 22, Power over Ethernet Introduction**. For configuration examples see **"PoE and PoE+ Configuration" on page 22.13**.

Policing

In **QoS**, once you have set-up your **Classification** and created your **Class maps**, you can start conditioning your traffic flows. One tool used for traffic conditioning is the policer (or meter). The principle of policing is to measure the data flow that matches the definitions for a particular class-map; then, by selecting appropriate data rates, allocate the flows into one of three categories, Red Yellow or Green. You then decide what action to apply to the Red, Yellow and Green data.

For more information see **"Policing (Metering) Your Data" on page 40.15**.

Policy maps

Policy maps are the means by which you apply your **Class maps** to physical switch ports. A policy map can be assigned to several ports, but a port cannot have more than one policy map assigned to it. See **QoS**.

For more information see **"Policy Maps" on page 40.10**.

Port bit map

An efficient method for the storage of a list of ports. Each port is represented by a single bit in a 32-bit or 64-bit value.

Port mirroring

Port mirroring enables traffic being received and transmitted on a switch port to be sent to another switch port, the mirror port, usually for the purposes of capturing the data with a protocol analyzer. The mirror port is the only switch port that does not belong to a VLAN, and therefore does not participate in any other switching. Before the mirror port can be set, it must be removed from all trunk groups and all VLANs except the default VLAN.

PPP

Point-to-Point Protocol. A data link protocol used to establish a direct connection between two networking nodes. PPP can provide connection authentication and transmission encryption. PPPoE (Point-to-Point Protocol over Ethernet) is used over broadband connections as is PPPoA (Point-to-Point Protocol over ATM) with DSL.

Premarking

In **QoS**, premarking relates to adding QoS markers to your incoming data traffic before it is metered. QoS markers can be applied at both the link layer (within the CoS field), and at the network layer (within the DSCP field). See **Policing**.

For more information see **"Premarking and Remarking Your Traffic" on page 40.11**.

Primary port

In **EPSR**, a ring port on the master node. This port determines the direction of the traffic flow, and is always operational.

For more information see **"Ring Components and Operation" on page 57.2**.

Provisioning

Stack member provisioning is the pre-configuration of **Stack member** position ready for insertion at a later time. Provisioning enables a network administrator to pre-configure vacant stack member capacity within a VCStack, ready to be hot-swapped in at a later time. Later, when the stack member switch is physically added, its configuration is automatically applied with the minimum network disruption.

For more information see **"Provisioning (Stack Members)" on page 81.20**.

Proxy ARP

Proxy ARP allows hosts that do not support routing (i.e. they have no knowledge of the network structure) to determine the physical addresses of hosts on other networks.

PSE

Power Sourcing Equipment. A device that can source power, such as an Ethernet switch, is termed Power Sourcing Equipment. Power Sourcing Equipment can provide power, along with data, over existing LAN cabling to Powered Devices (**PDs**). See **PoE**.

PSU

Power Supply Unit.

Q

Query Solicitation

Query Solicitation minimizes the loss of multicast data after a topology change on networks that use **EPSR** or spanning tree (**STP**, **RSTP**, or **MSTP**) for loop protection. Without Query Solicitation, when the underlying link layer topology changes, multicast data flow can stop for up to several minutes, depending on which port goes down and how much of the IGMP query interval remained at the time of the topology change. Query Solicitation greatly reduces this disruption.

For more information see **"Query Solicitation" on page 32.9**.

QoS

Quality of Service. QoS enables you to both prioritize traffic and limit its available bandwidth. The concept of QoS is a departure from the original networking protocols, in which all traffic on the Internet or within a LAN had the same available bandwidth. Without QoS, all traffic types are equally likely to be dropped if a link becomes oversubscribed. This approach is now inadequate in many networks, because traffic levels have increased and networks often carry time-critical applications such as streams of real-time video data. QoS also enables service providers to easily supply different customers with different amounts of bandwidth. Configuring Quality of Service involves two separate stages:

- Classifying traffic into flows, according to a wide range of criteria. Classification is performed by the switch's **Class maps**.
- Acting on these traffic flows.

For more information see **Chapter 40, Quality of Service (QoS) Introduction**.

Quality of Service

See **QoS**.

R

RADIUS

Remote Authentication Dial-In User Service. RADIUS is a networking protocol that provides centralized **AAA** (Authentication Authorization and Accounting) management for clients to a network. RADIUS is a client/server protocol that runs in the application layer, using UDP (User Datagram Protocol) for data transport. RADIUS authenticates users before granting them access to network resources and can account for the usage of network resources.

For more information see **Chapter 48, RADIUS Introduction and Configuration**. For configuration examples see **"RADIUS Configuration Examples" on page 48.15**.

Redistribute

Advertise routes learned from one routing protocol into another routing protocol.

Remarking

In **QoS**, remarking relates to adding QoS markers to your incoming data traffic after it is metered. QoS markers can be applied at both the link layer (within the CoS field), and at the network layer (within the DSCP field). See **Policing**.

Remote network MONitoring

See **RMON**.

Resiliency link

In VCStack, an extra, out-of-band, data link between stack members. In the event of loss of communication across the stacking connection, the stack members can determine the status of other members via communication on the resiliency link. This assists the stack members in deciding the correct course of action when communication on the stack is lost.

For more information see **"Stack Resiliency Link" on page 81.14**.

RIB

Routing Information Base. The RIB records all the routes that your device has learned. Your device uses the RIB to advertise routes to its neighbor devices and to populate the **FIB** (Forwarding Information Base).

For more information see **"RIB and FIB Routing Tables" on page 28.4**.

Ring port

In **EPSR**, a port that connects the node to the ring. On the master node, each ring port is either the primary port or the secondary port. On transit nodes, ring ports do not have roles.

For more information see **"Ring Components and Operation" on page 57.2**.

RMON

Remote Network MONitoring. RMON was developed by the IETF to support monitoring and protocol analysis of LANs with a focus on Layer 1 and 2 information in networks. RMON is an industry standard that provides the functionality in network analyzers. An RMON implementation operates in a client/server model. Monitoring devices (or 'probes') contain RMON agents that collect information and analyze packets. The probes are servers and the Network Management applications that communicate with them are clients.

For more information see **Chapter 72, RMON Introduction and Configuration**. For a configuration example see **"RMON Configuration Example" on page 72.3**.

Roaming Authentication

Roaming Authentication improves the usability of network security by enabling users to move within the network without requiring them to re-authenticate each time they move. If a supplicant (client device) moves from one wireless access point to another wireless access point, and the wireless access points are connected to different ports, then the switch (authenticator) recognizes that the supplicant has been authenticated and accepts the supplicant without requiring re-authentication.

For more information see **"Web-Authentication" on page 42.4**.

Root bridge

A single **Bridge** is selected to become the **Spanning tree's** unique root bridge. This is the device that advertises the lowest Bridge ID. Each bridge is uniquely identified by its Bridge ID, which comprises the bridge's root priority (a spanning tree parameter) followed by its MAC address.

For an overview of spanning tree operation see **"Spanning Tree Operation" on page 18.2**.

Root path cost

A **Spanning tree** property. Each port connecting a **Bridge** to a LAN has an associated cost, called the root path cost. This is the sum of the costs for each path between the particular bridge port and the **Root bridge**. The **Designated bridge** for a LAN is the one that advertises the lowest root path cost. If two bridges on the same LAN have the same lowest root path cost, then the switch with the lowest bridge ID becomes the designated bridge.

For an overview of spanning tree operation see **"Spanning Tree Operation" on page 18.2**.

RSTP

Rapid Spanning Tree Protocol. RSTP is an evolution of the Spanning Tree Protocol (**STP**) which provides for faster spanning tree convergence after a topology change. A device running RSTP is compatible with other devices running STP.

For more information see **"Rapid Spanning Tree Protocol (RSTP)" on page 18.8**. For a configuration example see **"Configuring RSTP" on page 18.9**.

S

SCP

Secure Copy Protocol. SCP allows for secure file transfer to and from the switch, protecting your network from unwanted downloads and unauthorized file copying.

For more information see **"Copying with Secure Copy (SCP)" on page 6.17**.

Script

A script is a sequence of commands stored as a plaintext file on a file subsystem accessible to the device, such as Flash memory. Each **Trigger** may reference multiple scripts and any script may be used by any trigger. When an event activates a trigger, the trigger executes the scripts associated with it in sequence. One script is executed completely before the next script begins.

See **Dynamic Link Failover**.

Secondary port

In **EPSR**, a second ring port on the master node. This port remains active, but blocks all protected VLANs from operating unless the ring fails. Similar to the blocking port in an STP/RSTP instance.

For more information see **"Ring Components and Operation" on page 57.2**.

SFTP

SSH File Transfer Protocol. SFTP provides a secure way to copy files onto your device from a remote device.

For more information see **"Copying with SSH File Transfer Protocol (SFTP)" on page 6.17**.

Software ACLs

See **ACL types**.

Spanning tree

A loop free portion of a network topology. The network topology is dynamically pruned to provide only one path for any packet. See **STP**, **RSTP** and **MSTP**.

Spanning Tree Protocol Root Guard

See **STP root guard**.

SSH

Secure Shell. SSH is a network protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides sessions between a host running a SSH server and a machine with a SSH client.

For more information see **Chapter 52, Secure Shell (SSH) Introduction**. For how to configure a SSH server see **"Configuring the SSH Server" on page 52.4**. For how to configure a SSH client see **"Configuring the SSH Client" on page 52.9**.

Stack

See VCStack.

Stack master

The switch that manages the stack, or VCStack, also referred to as the **Active master**.

See **Disabled master** for information about how this relates to **Stack master** or **Active master**.

Stack member

An individual switch that is part of a VCStack.

S-TAG

Service VLAN TAG.

Static aggregator

See **Static channel group**.

Static channel group

A static channel group, also known as a static aggregator, enables a number of ports to be manually configured to form a single logical connection of higher bandwidth. By using static channel groups you increase channel reliability by distributing the data path over more than one physical link.

Storm-control

Storm-control enables you to specify the threshold level for broadcasting, multicast, or destination lookup failure (DLF) traffic for a port. Storm-control limits the specified traffic type to the specified threshold.

For more information see **"Storm Control" on page 14.12**.

Storm protection

Storm protection uses **QoS** mechanisms to classify on traffic likely to cause a packet storm (broadcast and multicast). With QoS storm protection, several actions are possible when a storm is detected:

- You can disable the port physically.
- You can disable the port logically.
- You can disable the port for a particular VLAN.

For more information see **"Storm Protection" on page 40.24**.

STP

Spanning Tree Protocol. STP is the original bridge protocol defined by IEEE standard 802.1D-1988. It creates a single spanning tree over a network.

For more information see **"Spanning Tree Protocol (STP)" on page 18.5**. For a configuration example see **"Configuring STP" on page 18.6**.

STP root guard

Spanning Tree Protocol 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 on page 19.46.

Subnet address

A subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask.

Subnet mask

A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called address mask.

Superloop

Within an EPSR ring configuration, a superloop is a data loop whose path traverses more than a single EPSR ring. This occurrence is a fault condition that is usually do to a break in a physical segment that is shared by the two rings. For a superloop condition to occur, the two physical rings must share one or more data VLANs. Superloops can be prevented by employing Superloop Protection. For more information, See **"Superloop Protection" on page 57.18**.

Switch instance

A single switch chip with its associated ports, internal data interfaces, hardware tables, and packet buffer memory.

S-VID

Service VLAN ID.

S-VLAN

Service VLAN.

Synchronous

Transmission in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronized. This eliminates the need for start-stop elements, as in asynchronous transmission, but requires a flag character to be transmitted when there is no data to transmit. See **"Asynchronous" on page B.5**

T

TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) provides a method for securely managing multiple network access points from a single management service. TACACS+ is a TCP-based access control protocol that allows a device to forward a user's username and password to an authentication server to determine whether access can be allowed. In addition to this authentication service, TACACS+ can also provide authorization and accounting services. One of the features of TACACS+ is the ability to separate authentication, authorization and accounting so that these functions can be provided independently on separate servers.

For information on the AlliedWare Plus implementation of TACACS+, see **Chapter 50, TACACS+ Introduction and Configuration** and **Chapter 51, TACACS+ Commands**.

TCN

Topology Change Notification.

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.

For more information see **"Thrash Limiting" on page 14.14**

TLV

Type-Length-Value. A single **LLDPDU** contains multiple TLVs. TLVs are short information elements that communicate complex data, such as variable length strings, in a standardized format. Each TLV advertises a single type of information, such as its device ID, type, or management addresses. See **LLDP advertisements**.

Traceroute

Traceroute is used to discover the route that packets pass between two systems running the IP protocol. Traceroute sends an initial UDP packets with the Time To Live (TTL) field in the IP header set starting at 1. The TTL field is increased by one for every subsequent packet sent until the destination is reached. Each hop along the path between two systems responds with a TTL exceeded packet (ICMP type 11) and from this the path is determined.

Transit node

In **EPSR**, nodes other than the master node in the domain.

Transit node states are:

- Idle - the state when EPSR is first configured, before the master node determines that all links in the ring are up. In this state, both ports on the node are blocked for the data VLAN. From this state, the node can move to Links Up or Links Down.
- Links Up - the state when both the node's ring ports are up and forwarding. From this state, the node can move to Links Down.
- Links Down - the state when one or both of the node's ring ports are down. From this state, the node can move to Preforwarding.
- Pre-forwarding - the state when both ring ports are up, but one has only just come up and is still blocked to prevent loops. From this state, the transit node can move to Links Up if the master node blocks its secondary port, or to Links Down if another port goes down.

For more information see **"Ring Components and Operation" on page 57.2**.

Tri-authentication

Authentication commands enable you to specify three different types of device authentication: **802.1X** authentication, **MAC authentication**, and **Web-authentication**. All three types can be configured to run simultaneously on a switch port. The simultaneous configuration and authentication of all three types on a port is called tri-authentication.

For a configuration example see **"Tri-Authentication Configuration" on page 42.25**.

Trigger

A trigger is an ordered sequence of scripts that is executed when a certain event occurs. Each trigger may reference multiple scripts and any **Script** may be used by any trigger. When an event activates a trigger, the trigger executes the scripts associated with it in sequence. One script is executed completely before the next script begins.

See **Dynamic Link Failover**.

Type-Length-Value

See **TLV**.

U

Unicast

Two individual devices hold a conversation just between themselves.

V

VCStack

A group of two or more switches operating as a single switch. See **Virtual Chassis Stacking**.

VCStack fast failover

VCStack Fast Failover provides absolutely minimal network downtime in the event of a problem with the stack.

See the **reboot rolling** command on page 82.4.

VID

VLAN Identifier or VLAN ID. When you create a VLAN you give it a numerical VID which is included in VLAN-tagged Ethernet frames to and from this VLAN.

Virtual Chassis Stacking

Virtual Chassis Stacking (VCStack™) is the name given to two or more Allied Telesis switches that are configured to operate as a single switch. From a configuration and management point of view, it is as though the switches are just one device with a seamless transition from the ports of one stack member to the ports of the next.

For more information see **Chapter 81, VCStack Introduction**.

VLAN classification

A packet can be allocated VLAN membership based on its protocol, subnet, or port.

VLAN ID

See **VID**.

VLAN identifier

See **VID**.

VLAN tag

IEEE standard 802.1q defines an additional 4 byte tag field that can be inserted immediately following the MAC address, plus any routing fields present. This field contains a 12 bit VLAN identifier, commonly referred to as the VLAN tag. The VLAN tag is used to determine which VLAN a given frame should be forwarded to.

Other tags included in the 802.1q tag field is a Tag Protocol Identifier tag, and a Type of Service tag used to determine data priority.

Voice VLAN

Voice VLAN automatically separates voice and data traffic into two different VLANS. This automatic separation places delay-sensitive traffic into a voice-dedicated VLAN, which simplifies QoS configurations.

For more information see **"Voice VLAN" on page 69.3**.

VoIP

Voice over Internet Protocol. Enables the delivery of voice communications over IP networks such as the Internet or other packet-switched networks instead of over traditional telephony circuits.

W

Web-authentication

The switch sends a login screen to the client webbrowser which must be authenticated before access is granted to the network. See **AAA** and **Tri-authentication**.

For a sample configuration script see **"Sample Web-Authentication Configuration" on page 44.9**.

Wildcard mask

A subnet mask in which bits set to 0 indicate an exact match and bits set to 1 indicate 'don't care'.